НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ

КАФЕДРА СИСТЕМНОГО ПРОГРАМУВАННЯ І
СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ

«На правах рукопису»
УДК 004.056.53

«До захисту допущено»

Завідувач кафедри СПСКС

_____ В.П.Тарасенко
(підпис) (ініціали, прізвище)

"___"_____2018р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 123 Комп'ютерна інженерія
Системне програмування

на тему: Засоби аутентифікації об'єктів мережі на основі аналізу фізичних параметрів сигналів

Виконала: студентка ІІ курсу, групи КВ-62м

Тупарєва Валентина Андріївна _____ _____
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник доцент, к.т.н, Тарасенко-Клятченко О.В. ____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет прикладної математики

Кафедра системного програмування і спеціалізованих комп'ютерних систем

Рівень вищої освіти – другий (магістерський)
Спеціальність 123 Комп'ютерна інженерія
Системне програмування

ЗАТВЕРДЖУЮ
Завідувач кафедри СПСКС
_____
_В.П.Тарасенко__
(підпис) (ініціали, прізвище)
«___»_____2018р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Тупарєвої Валентини Андріївни
(прізвище, ім'я, по батькові)

1. Тема дисертації: ЗАСОБИ АУТЕНТИФІКАЦІЇ ОБ'ЄКТІВ МЕРЕЖІ НА ОСНОВІ АНАЛІЗУ ФІЗИЧНИХ ПАРАМЕТРІВ СИГНАЛІВ,
науковий керівник дисертації Тарасенко-Клятченко Оксана Володимирівна, к.т.н., доцент,
затверджені наказом по університету від «22» березня 2018 р. №986-с

2. Термін подання студентом дисертації 11 травня 2018 р.

3. Об'єкт дослідження: забезпечення інформаційної безпеки у безпроводових комп'ютерних мережах.

4. Предмет дослідження: способи аутентифікації об'єктів мережі.

5. Перелік завдань, які потрібно розробити:
- провести аналіз існуючих методів аутентифікації

- зробити порівняльний аналіз існуючих алгоритмів аутентифікації
- розробка модифікації алгоритму аутентифікації користувачів на основі оцінки параметрів каналу зв'язку

6. Перелік ілюстративного матеріалу: блок-схема модифікованого алгоритму аутентифікації, організація WI-FI мережі, схема алгоритму аутентифікації з загальним ключем, блок-схема алгоритму аутентифікації за допомогою біометричних характеристик, системи ідентифікації та аутентифікації, схема алгоритму аутентифікації за PIN-кодом.

7. Перелік публікацій:

-X наукова конференція магістрантів та аспірантів «Прикладна математика та комп'ютинг» ПМК-2018;

- 20-th International conference on System Analysis and Information Technology SAIT 2018, May 21–23, 2018.

8. Дата видачі завдання 5 вересня 2016 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Ознайомлення з предметною областю дослідження.	20.11.2016	
2	Визначення структури магістерської дисертації; вивчення літератури, пошук додаткової літератури.	11.04.2017	
3	Робота над першим розділом магістерської дисертації	27.05.2017	
4	Проведення наукового дослідження; робота над другим розділом магістерської дисертації	04.10.2017	
5	Проведення наукового дослідження; робота над третім розділом магістерської дисертації	11.12.2017	
6	Проведення наукового дослідження; підготовка матеріалів доповіді на конференції ПМК-2018	10.02.2018	
7	Завершення роботи над основною частиною магістерської дисертації; підготовка ілюстративного матеріалу	05.04.2018	
8	Оформлення текстової і графічної частини магістерської дисертації	20.04.2018	
9	Попередній розгляд магістерської дисертації на кафедрі	26.04.2018	

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _____
(підпис) (ініціали, прізвище)

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

IP – Internet Protocol – мережевий протокол;
EAP — протокол розширеної аутентифікації (Extensible Authentication Protocol);
MAC-адреса - Media Access Control - унікальний ідентифікатор, який присвоюється кожній одиниці активного обладнання;
MIC — технологія перевірки цілісності повідомлень (Message Integrity Check); TKIP — протокол інтеграції тимчасового ключа (Temporal Key Integrity Protocol);
VPN- Virtual Private Network — віртуальна приватна мережа;
WPA — технологія захищеного доступу до безпроводових мереж.

ВСТУП

Бездротові мережі займають особливе місце в житті сучасного суспільства. Вони знайшли широке застосування в повсякденному житті. Популярність і динаміка розвитку бездротових технологій обумовлена їх зручністю і широкою сферою застосування. Незважаючи на відносну молодість бездротових мереж, в даний час існує безліч технологій, стандартів і рішень, що дозволяють забезпечувати безпечну і високошвидкісну передачу даних по бездротових каналах зв'язку. Як і у всіх системах передачі даних, важливою характеристикою є безпека інформації, що передається, в якій необхідно бути впевненим в тому, що повідомлення дійшло до адресата без перехоплення і змін. Звідси випливають вимоги, що пред'являються до процесу забезпечення інформаційної безпеки (ІБ). ІБ повинна забезпечувати цілісність, доступність і конфіденційність інформації.

Під поняттям конфіденційності ми розуміємо те, що наша особиста або ділова інформація не повинна бути доступна третім особам. При використанні інформаційних систем (ІС), що мають на увазі будь-які взаємини між декількома суб'єктами, ми хочемо, щоб ніхто не міг робити ніяких дій від нашого імені. Для вирішення цих завдань використовуються складні криптографічні системи, що забезпечують надійне шифрування даних, і створення неподделиваемих цифрових підписів. З розвитком систем забезпечення інформаційної безпеки фактор неправильної роботи ІС відходить на другий план. Більшість загроз ІБ пов'язане з людським фактором. З більшістю ІС може працювати кілька

користувачів, а, отже, необхідно розмежувати доступ до ІС. Для цієї мети використовують різні методики поділу доступу. Поділ доступу має на увазі три процедури взаємодії між суб'єктом і системою: ідентифікація, аутентифікація і авторизація. На етапі ідентифікації відбувається визначення особистості, під час аутентифікації відбувається підтвердження особи, а при проведенні

авторизації з'ясовується до яких ресурсів ІС, отримує доступ конкретний користувач. Найбільш слабкою ланкою в даній ланцюжка є аутентифікація. При зломі системи аутентифікації зловмисник буде сприйнятий системою як легальний користувач і йому будуть розкриті дані зберігаються в ІС. На етапі аутентифікації відбувається взаємодія між людиною і комп'ютерною системою.

1. АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА ОБГРУНТУВАННЯ ТЕМИ ДИПЛОМНОГО ПРОЕКТУ

1.1. Аналіз існуючих методів аутентифікації

Аутентифікація - це процедура перевірки автентичності користувачів. Механізми аутентифікації засновані на трьох факторах: знаннях, зберіганні і біометрії.

Користувач отримує доступ тільки після оцінки одного або декількох наступних параметрів:

- код користувача та пароль;
- IP-адреса;
- Біометричні дані;
- Місцезнаходження.

Тим самим, після цього ми можемо вирішити, чи є користувач легальним чи ні. Отже, ми можемо забезпечити більш високий рівень безпеки.

Доступ може бути надано тільки тоді, коли людина знаходиться в своє місцезнаходження і коли конкретний сервер знаходиться в режимі онлайн. Інакше, доступ буде заборонений. Іншими словами, інформація не повинна бути поширена за межами цього приміщення. У таких випадках, існуючі засоби безпеки є недостатніми для забезпечення рівня безпеки.

1.2. Аутентифікація за допомогою паролів

Найпростішим способом аутентифікації є текстовий число-буквений пароль. Користувача комп'ютерної системи просять ввести ім'я облікового запису та пароль. Систему цього типу легко реалізувати і тому ваона отримала повсюдне поширення.

Метод аутентифікації по паролю є найстарішим і простим (Рисунок 1.1).

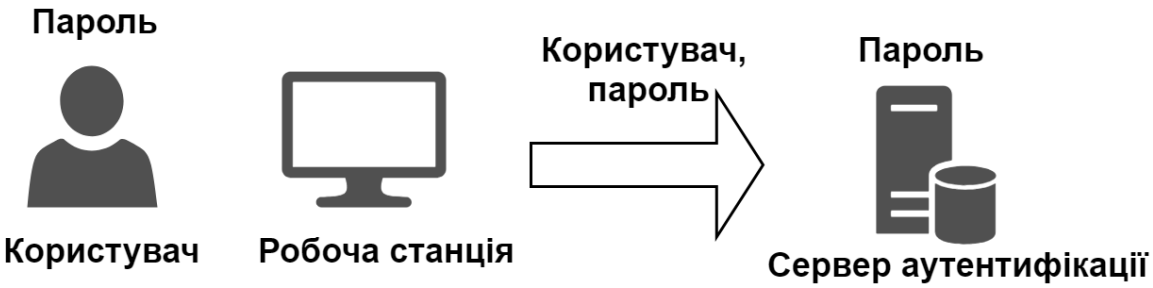


Рисунок 1.1 - Аутентифікація за паролем

Аутентифікація відбувається за наступним алгоритмом:

- Користувач вводить свої дані (ім'я та пароль),
- Дані передаються на сервер аутентифікації,
- Сервер аутентифікації звіряє отримані дані з даними в базі даних. Якщо дані збігаються, користувач проходить аутентифікацію успішно.

1.3. Аутентифікація на основі хеш – ключа

Недоліком використання аутентифікації за паролем є те, що він може бути перехоплений в радіоканалі. Тому, у даному методі аутентифікації, пароль передається не у відкритому вигляді, а хешується разом з випадковим числом.

Хеш-функція – це перетворення, що відображає множину усіх двійкових послідовностей X довжини n в множину двійкових послідовностей Y довжини b, де b < n (Рисунок 1.2).

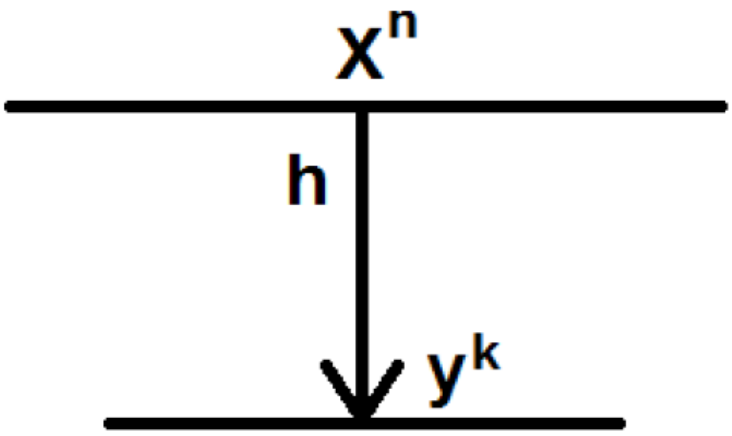


Рисунок 1.2 - Перетворення хеш-функції

Алгоритм проходження аутентифікації на основі хеш - ключа (Рисунок 1.3).

- Користувач вводить свої дані (ім'я та пароль) на робочій станції.
- Робоча станція обчислює хеш-функцію від введеного пароля і випадкового числа. Ім'я користувача і хеш-функція передаються на сервер аутентифікації.
- Сервер аутентифікації порівнює значення, отримане від користувача зі значенням хеш-функції обчисленої з випадкового числа і пароля. Якщо дані збігаються, то аутентифікація проходить успішно.

Головною перевагою односпрямованої хеш-функції є неможливість відновити вихідну інформацію при знанні хеш-функції. Тому, якщо порушник отримає доступ до бази даних сервера аутентифікації, то він не зможе відновити паролі з бази даних хеш-функцій.

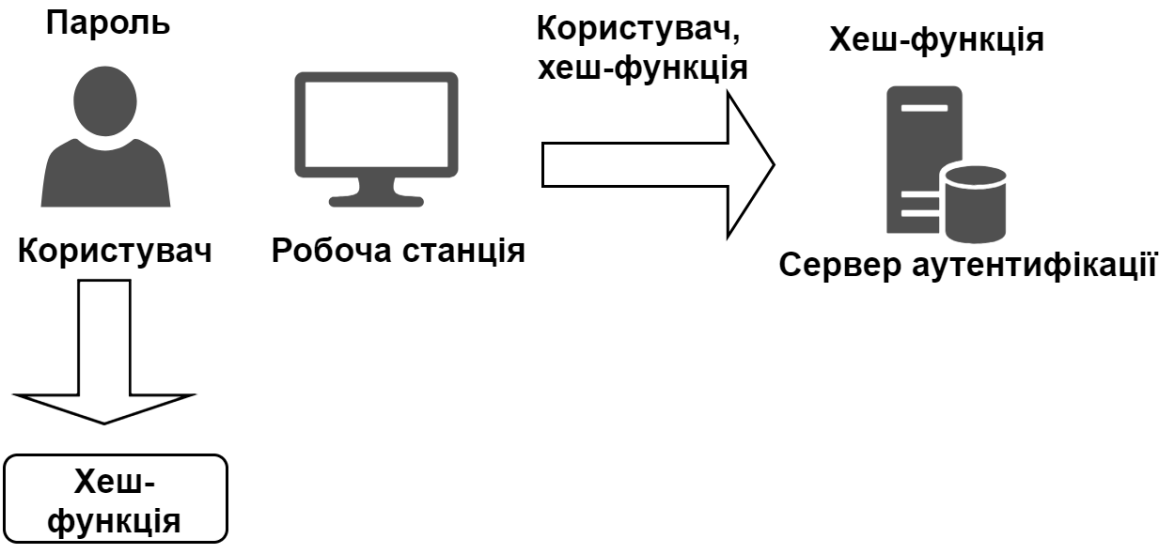


Рисунок 1.3 - Аутентифікація на основі хеш-ключа

1.4. Аутентифікація на основі PIN – коду

PIN – код (PersonalIdentificationNumber) - це різновид пароля, який використовується для аутентифікації на локальному пристрої. Різниця PIN-коду та паролю полягає в різних умовах та сферах використання.

Характеристики використання PIN-коду:

- Не можна ввести PIN-код без використання клавіатури даного пристрою.
- PIN-код не передається по мережі і не може бути перехоплений.
- Використання терміну «PIN-код» як термін «пароль» неправильно, тому що аутентифікація по PIN-коду використовує багатофакторну аутентифікацію.

Однак, вище зазначені методи аутентифікації за допомогою пароля мають ряд серйозних недоліків. Наприклад, користувачі схильні до вибору простих паролів, які можуть бути легко зламані або навіть вгадані.

Відповідно до недавніх досліджень, команда фахівців з інформаційної безпеки, після запуску в одній великій корпоративній мережі мережевого зломщика паролів, через 30 секунд отримала близько 80% всіх паролів.

Для вирішення проблеми небезпечних паролів на деяких підприємствах вводять політики безпеки, що регламентують складність паролів.

Наприклад, від усіх співробітників можуть зажадати ставити паролі довжиною не менше 8 символів і складаються не менше ніж з трьох груп символів. Але складні паролі призводять до іншої проблеми - вони складні для запам'ятовування. Це призводить до того, що паролі часто забувають або записують на папір.

Таким чином, виходить, що безпечні паролі складно запам'ятати, а запам'ятовуються паролі, як правило, легко зламуються.

Схожа проблема виникає і в разі створення безлічі облікових записів. Практично кожна інформаційна система вимагає від нас створення облікового запису, а відповідно і введення пароля.

Як правило, користувач або використовує один і той же пароль кілька разів в різних системах, або використовує різні паролі, але зберігає їх в одному місці, наприклад, на аркуші паперу, мобільному телефоні або спеціалізованій базі даних. Обидва методи пов'язані з ризиком.

У першому випадку, коли один пароль використовується в різних системах, в разі компрометації пароля зловмисник отримує доступ до інших облікових записів. У другому випадку, зловмисник може спробувати отримати доступ до бази паролів.

Існують спеціальні системи, що впроваджуються в корпораціях, що дозволяють користувачеві отримувати доступ до безлічі комп'ютерних

систем з використанням одного пароля. Прикладами таких систем є Kerberos, Windows Live ID, RSA Sign-On Manger, OpenSSO.

Дані системи забезпечують високий рівень безпеки. Але, як і у випадку з базою паролів, скомпрометований пароль відкриє зловмисникові доступ відразу до всіх ресурсів.

Відзначимо, що деякі комп'ютерні системи, для поліпшення безпеки вимагають часту зміну пароля. Пароль, який часто змінюють, складніше зламати «грубою силою», адже подібні атаки вимагають часу.

Якщо атакуючий не встигне зламати пароль вчасно, то зламаний в результаті пароль може виявитися недійсним. Але чим частіше пароль змінюється, тим його складніше запам'ятати.

Якщо взяти окремого користувача комп'ютерних систем, ціна забутого пароля дуже мала. У разі забування пароля співробітник зв'язується зі службою технічної підтримки і попросить змінити пароль на новий.

Багато систем дозволяють скидати свій пароль в разі правильної відповіді на спеціальне питання, наприклад, дівоче прізвище матері або ім'я домашнього вихованця.

Нижче розглянемо кілька основних видів атак і методи їх захисту:

- Крадіжка парольного файлу: порушник може отримати пароль з парольного файлу або з резервної копії.

Захист: хешування пароля.

- Примус: порушник може змусити користувача відкрити свій пароль шляхом погроз або фізичного примусу.

Захист: сигнал про примус, тобто при вході в систему користувач вводить не свій пароль, а так званий пароль «вхід під примусом», який повідомить систему про те, що користувач входить в систему під примусом.

- Підглядання: знаходиться поруч порушник або відеокамера стежать, як користувач вводить пароль.

Захист: невідображення пароля, тобто відображення пароля на екрані незначущими символами / іншою кількістю символів, використання стираючих систем стійких до атаки підглядання, а також використання певної кількості часу для входу в систему.

- Трасування пам'яті: порушник використовує програму для копіювання пароля з буфера клавіатури.

Захист: захист пам'яті, деякі ОС використовують апаратний захист буферів клавіатури.

1.5. Аутентифікація за допомогою OTP паролів

Одноразові паролі (OTP - One-timepassword) - динамічна аутентифікаційна інформація, що генерується для одиничного використання за допомогою аутентифікаційних пристроїв (програмних або апаратних).

OTP стійкий до атак, в ньому аналізується мережевий трафік. Це є більш надійно ніж паролі, що запам’ятовуються. Незважаючи на те, що у порушника є можливість дізнатися пароль, аналізуючи мережевий трафік, пароль дійсний один раз і протягом певного часу.

В якості можливих пристроїв для генерації одноразових паролів зазвичай використовуються OTP токени.

OTP токен - мобільний персональний пристрій, що належить користувачеві. Він використовує одноразові паролі для аутентифікації. Отже, така аутентифікація в порівнянні з парольною, і є аутентифікацією за допомогою іншого фактора аутентифікації - «на основі володіння чимось».

Ще один пріоритет застосування аутентифікаційних пристроїв це те, що більшість з них вимагають від користувача використання PIN-коду:

- Для активації OTP-токена;
- в якості додаткових даних, що використовуються при генерації OTP;
- для пред'явлення сервера аутентифікації разом з OTP.

Якщо додатково застосовується ще і PIN-код, в методі аутентифікації використовуються два фактори аутентифікації, тобто даний метод відноситься до багатофакторної аутентифікації.

Проходження двофакторної аутентифікації з використанням одноразових паролів:

1. Користувач вводить username / password;

2. Пара username / password передаються на сервер аутентифікації;

3. Сервер аутентифікації виробляє перевірку введених користувачем даних;

4. При успішному виконанні пункту 3, сервер генерує запит на одноразовий пароль або передає користувачеві на пристрій вже згенерований;

5. Користувач вводить одноразовий пароль і передає його на сервер;

6. Сервер виробляє перевірку подібності паролів;

7. При успішному виконанні пункту 6, аутентифікації вважається успішною.

В якості основних джерел одноразових паролів, які використовуються в веб-додатках, можна виділити:

1. Програмні токени, що генерують одноразові паролі на підставі секретного ключа, введеного в них, і поточного часу. Секретні ключі користувачів, які є фактором володіння, зберігаються на сервері, що дозволяє виконати перевірку одноразових паролів.

2. Випадково генеруються коди, що передаються користувачеві через SMS або інший канал зв'язку. Фактором володіння тут виступає SIM-карта користувача, прив'язана до певного номера.

3. Scratch card або роздруківка зі списком заздалегідь сформованих одноразових паролів. Кожен новий вхід в систему вимагає введення нового одноразового пароля з зазначеним номером.

1.5. Методи аутентифікації за допомогою OTP паролів

Найчастіше в OTP-токенах застосовується симетрична криптографія. Пристрій кожного користувача має унікальний персональний секретний ключ, застосовуваний для шифрування даних (в залежності від реалізації методу) для генерації OTP. Цей же ключ зберігається на сервері аутентифікації.

Сервер шифрує дані і порівнює два результату шифрування: отриманий ним і відправлений від клієнта. Якщо результати ідентичні, то користувач успішно проходить аутентифікацію. OTP-токени, що використовують симетричну криптографію, можуть працювати в асинхронному або синхронному режимі. Тому методи, використовувані OTP-токенами, можна розділити на дві групи, що працюють:

- в асинхронному режимі («запит-відповідь»);
- в синхронному режимі («тільки відповідь»).

У методі «запит-відповідь» OTP є відповіддю користувача на випадковий запит від сервера аутентифікації (Рисунок 1.4).

Рисунок 1.4 - Метод «Запит-відповідь»

Приклад аутентифікації користувача при використанні OTP-токеном методу «запит-відповідь»:

- Користувач вводить ім'я користувача;
- Ім'я користувача передається по мережі у відкритому вигляді;
- Сервер аутентифікації генерує випадковий запит (наприклад, «34256781»);
- Запит передається по мережі у відкритому вигляді;
- Користувач вводить запит в свій OTP-токен;
- OTP-токен шифрує запит за допомогою секретного ключа користувача («weretrer»), в результаті виходить відповідь («87235416»), який відображається на екрані OTP-токена;
- Користувач вводить цей відповідь на робочої станції;
- Відповідь передається по мережі у відкритому вигляді;
- Сервер аутентифікації знаходить запис користувача в базі даних і за допомогою закладеного їм секретного ключа користувача зашифровує той же запит;

- Сервер порівнює представлений відповідь від користувача («8723546») з обчисленим їм самим відповіддю («8723546»);
- При збігу значень аутентифікація вважається успішною.

У методі «тільки відповідь» пристрій аутентифікації і сервер аутентифікації генерують «прихований» запит, використовуючи значення попереднього. Для ініціалізації даного процесу використовується унікальне випадкове число, що генерується при ініціалізації OTP-токена.

Приклад аутентифікації користувача при використанні OTP-токена методу «тільки відповідь» (Рисунок 1.5):

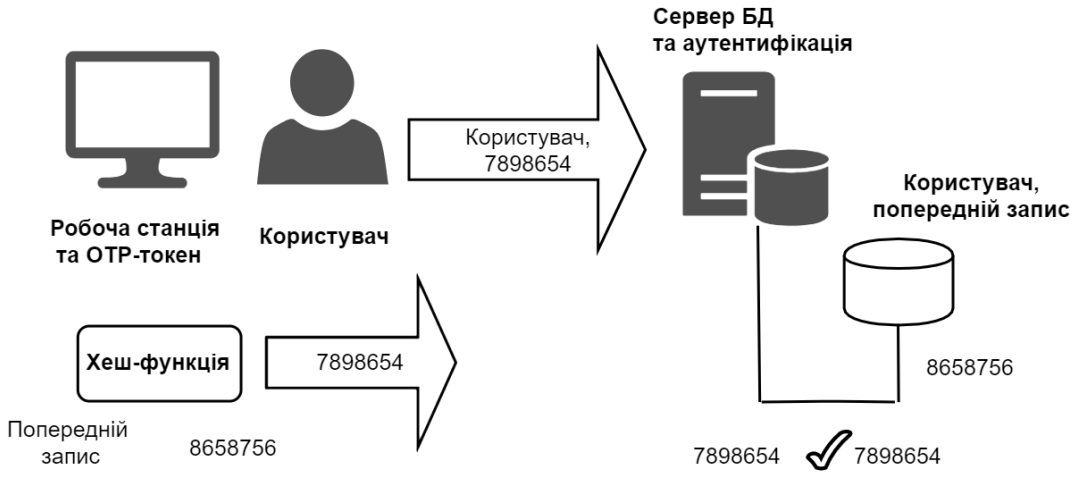


Рисунок 1.5 - Метод «Тільки відповідь»

- Користувач активує OTP-токен, який обчислює і відображає відповідь на «прихований» запит;
- Користувач вводить ім'я користувача і відповідь «8658756»;
- Ім'я користувача і відповідь передаються по мережі у відкритому вигляді;

- Сервер знаходить запис і генерує такий же прихований запит і шифрує його на основі секретного ключа користувача, отримуючи відповідь на свій запит;

- Якщо обчислений відповідь збігається з відповіддю користувача, то аутентифікація вважається успішною.

Методи аутентифікації за допомогою OTP-паролів мають ряд недоліків таких, як підбір, вгадування, крадіжка пароля і т.д. Нижче розглянемо кілька основних видів атак і методи їх захисту:

- Атака «Людина посередині». Перехоплення пароля при аутентифікації, блокування законного користувача і використання порушником перехопленого пароля для входу в систему.

Захист: використання методу «запит-відповідь»

- Крадіжка токена аутентифікації.

Захист: PIN-коди в токенах аутентифікації. Вимога введення PIN-коду перед початком генерації OTP.

При використанні програмних токенов аутентифікації, підтверджується справжність робочої станції, а не користувача. Навіть якщо при використанні аутентифікації по PIN-коду багатофакторна аутентифікація замінюється на Однофакторні.

Будь-якому користувачеві, що має фізичний доступ до станції, необхідно тільки дізнатися PIN-код. Цей метод ефективний тільки для співробітників, що працюють вдома.

1.6. Аутентифікація за допомогою біометричних характеристик

Біометрія - це ідентифікація людини по унікальним, властивим тільки йому біологічними ознаками. Тобто, можна сказати, що біометричні технології спочатку розроблялися для точного встановлення особи людини. І рішення використовувати їх в області інформаційної безпеки виглядає цілком логічним. Причому даний напрямок розвиває дуже активно.

Сьогодні експлуатується вже більше десятка різних біометричних ознак. Для найпоширеніших з них (відбитки пальців і райдужна оболонка очей) існує безліч різних за принципом дії сканерів. Тому користувачам, які вирішили використовувати біометричну аутентифікацію, є з чого вибрати.

З огляду на те, що біометрична характеристика унікальна для кожної людини, його можна використовувати для однофакторной аутентифікації. Її можна використовувати спільно з іншим методом аутентифікації для забезпечення багатофакторної аутентифікації.

Такий метод аутентифікації досить простий в проходженні для користувачів. Добре спроектований метод просто знімає біометричний параметр з людини і виконує аутентифікацію.

Біометричні показники діляться на:

- Фізіологічні (фізичні, статичні): характеристики, засновані на даних, отриманих шляхом вимірювання анатомічних характеристиках людини;
- Поведінкові (динамічні): характеристики, засновані на даних, отриманих шляхом вимірювання дій людини. Основним параметром поведінкової характеристики є протяжність в часі - вимірюється дію має початок і кінець.

Приклади фізіологічних характеристик:

- Райдужна оболонка ока;
- Сітківка ока;
- Відбиток пальця;
- Геометрія руки і обличчя.

Приклади поведінкових характеристик:

- Голос;
- Підпис.

Відмінності між цими двома характеристиками полягають в тому, що поведінкові біометричні параметри залежать від фізіології людини, наприклад, голос залежить від форми зв'язок, підпис від спритності призначених для користувача рук, поведінка людини від його характеру. Ці характеристики можуть змінюватися протягом часу і вплинути на ефективність роботи пристрою аутентифікації.

Фізіологічні характеристики не змінюються з плином часу. Але на відміну від поведінкових характеристик, вони можуть здатися більш болючими. З точки зору безпеки найбільш ефективною є біометричні характеристики.

Такі системи працюють однаково, але при цьому розрізняються об'єктами і способами вимірювань.

Алгоритм робота біометричної системи (рисунок 6):

- Користувач надає зразок (приклад поведінкової або фізіологічної характеристики / чітке опознаваемое зображення);
- Реєструючий пристрій обробляє зразок і перетворює його в контрольний шаблон (велика числова послідовність). Цей зразок не можна відновити з шаблону;
- Контрольний шаблон порівнюється з еталонним шаблоном. Еталонний шаблон береться з бази даних. Так як, ці два параметри не збігаються один з одним повністю, то система виносить рішення про достатню збігу. Ступінь збігу повинна перевищувати величину, звану граничним значенням.

Однак, біометрична система не ідеальна і може приймати помилковий контрольний шаблон за істинний. Точність біометричної системи визначається наступними параметрами:

- Помилка типу I: коефіцієнт невірних збігів (FMR) або ймовірність (FAR);

- Помилка типу II: коефіцієнт невірних розбіжностей (FNMR) або ймовірність помилкового відмови в доступі (FRR).

Обидва коефіцієнта обмежують вхід авторизованим користувачам.

Головною перевагою біометричних технологій є висока надійність. І дійсно, всі знають, що двох людей з однаковими відбитками пальців в природі не існує. Правда, сьогодні вже відомо кілька способів обману дактилоскопічних сканерів [8].

Наприклад, потрібні відбитки пальців можуть бути перенесені на плівку або до пристрою може бути прикладена велика фотографія пальця зареєстрованого користувача. Втім, треба зізнатися, що сучасні пристрої вже не попадаються на такі прості прийоми.

Так що зловмисникам доводиться вигадувати все нові і нові способи обману біометричних сканерів, багато з яких вимагають роботи висококласних фахівців і дуже дорогого обладнання [7].

Ще однією перевагою біометричних систем аутентифікації є відсутність пароля як такого. Користувачеві не треба нічого запам'ятовувати і його пароль завжди з собою.

Спочатку системи біометричної аутентифікації, коштували дорого, займали багато місця і повільно працювали. Тому їх застосовували тільки в системах з особливо важливою інформацією. Але з часом обладнання стало дешевше, зменшилися габарити і стали працювати набагато швидше.

Біометричні системи вимагають порівняння спочатку зареєстрованого еталона біометричної інформації з новим, перевіряється зразком.

Завдяки простоті створення і зручності користування найбільшого поширення набули сканери відбитків пальців. В даний момент на ринку існує величезна кількість ноутбуків і комп'ютерних периферійних

пристроїв, які використовують сканери відбитків пальців для аутентифікації користувачів.

Серед рішень існують USB-flash карти і зовнішні жорсткі диски. Вважається, що біометричні системи аутентифікації на сьогоднішній день забезпечують найвищий рівень безпеки.

Тим не менш, вони також мають ряд недоліків, що перешкоджають їх повсюдного впровадження:

- Потрібно додаткове апаратне забезпечення;
- Устаткування потребує постійного контролю і технічного обслуговування, відсутні;
- Деякі види біометричних паролів (наприклад, відбитки пальців), відносно легко крадуться і можуть бути підроблені;
- Складність впровадження в системах віддаленої аутентифікації, наприклад, в інтернет. Потрібна наявність біометричного датчика заслуговує на довіру;
- Неможливість застосування людям (інвалідам), що мають фізичні вади.

Атаки на біометричні системи і захист від них:

- Підробка відмінною риси, порушник зможе виготовити копію фізичної відмінною риси і надає цей параметр датчику.

Захист: зняття показників з високим рівнем деталізації, тобто при виготовленні еталонного шаблону знімають також додаткові біометричні характеристики.

- Відтворення користувача, порушник записує поведінкову рису людини і відтворює на датчику.

Захист: змінне поведінки, система буде вимагати різні прояви поведінкового характеру і просто запис приймати не буде.

- Перехоплення біометричних показників.

Захист: шифрування біометричних показників, в якому система буде шифрувати дані і після цього передавати).

1.7. Способи аутентифікації в бездротових мережах

Існує безліч способів аутентифікації, що було проаналізовано нижче.

Аутентифікація електронним підписом може бути декількох типів, які описані нижче.

- Простий електронний підпис – він, використовуючи код, паролю або інших засобів, затверджує його створення деякою людиною;
- некваліфікований електронний підпис - він:
  - -отримано за допомогою криптографічної зміни інформації за допомогою використання ключа;
  - визначає людину, яка підписала електронний документ;
  - виявляє факт внесення змін до електронного документу після моменту його підписання;
  - створюється з використанням засобів електронного підпису.
- кваліфікований електронний підпис - такий, що відповідає всім ознакам некваліфікованої електронної підпису і включає ключ його перевірки, який вказано в кваліфікованому сертифікаті, а також засоби, що одержали підтвердження відповідності вимогам.

Алгоритм, який використовується при даній аутентифікації:

1. Користувач вводить username / password;

2. Пара username / password передаються по мережі у відкритому вигляді;

3. Сервер аутентифікації виробляє пошук облікового запису в базі даних і порівнює введені даних з її вмістом;

4. У разі збігу даних аутентифікація вважається успішною.

IEEE 802.11x передбачає використання двох методів аутентифікації:

- відкрита аутентифікація OA (Open Authentication);
- аутентифікація з загальним ключем SKA (Shared Key Authentication).

Відкрита аутентифікація

Відкрита аутентифікація (OA) [1] представляє собою алгоритм з нульовою авторизацією. Точка доступу приймає будь-який запит на аутентифікацію.

Контроль доступу при відкритій аутентифікації здійснюється з використанням заздалегідь сконфігурованого WEP-ключа (Wired Equivalent Privacy) у точці доступу (K1) і на клієнтській станції (K2). Ця станція і точка доступу повинні мати однакові ключі, тоді вони можуть зв'язуватися між собою. Якщо K1 не дорівнює K2, фрейм буде відкинутий через розбіжності ключів (рис. 1.6).

Рис. 1.6 - Процес відкритої аутентифікації при відмінності WEP-ключів

Основним недоліком методу відкритої аутентифікації є те, що точка доступу не має можливості перевірити правомочність клієнта; відсутність такої можливості є суттєвим недоліком системи захисту, якщо в безпроводовій локальної мережі не використовується WEP-шифрування.

Аутентифікація з загальним ключем (SKA)

Для організації аутентифікації з загальним ключем (SKA) [1] необхідно налаштувати статичний ключ шифрування алгоритму WEP. Клієнт робить запит в точку доступу на аутентифікацію, та в разі можливості доступу, отримує підтвердження, яке містить 128 байт випадкової інформації.

Станція шифрує дані, які получила від точки доступу, алгоритмом WEP (проводиться побітове додавання по модулю 2 даних повідомлення з послідовністю ключа) і відправляє зашифрований текст разом із запитом на доступ. Точка доступу розшифровує текст і порівнює з відкритим текстом. Якщо значення збігаються, то точка доступу посилає клієнту підтвердження з'єднання, в іншому випадку - відмовляє (рис. 1.7).

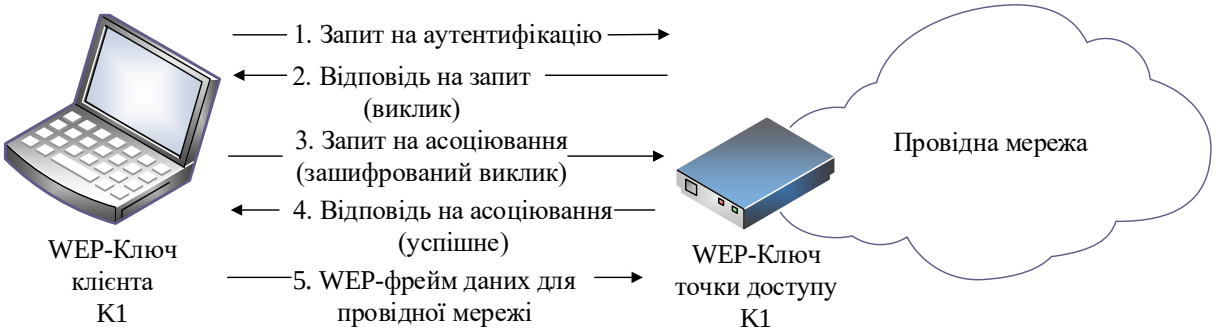


Рис.1.7 - Процес аутентифікації з ключем, що спільно використовується

Основним недоліком методу аутентифікації з загальним ключем (SKA) є те, що проаналізувавши досить великий обсяг трафіку мережі (3-7 млн пакетів), можна обчислити ключ шифрування.

На заміну застарілого WEP протоколу прийшов протокол WPA, що є більш надійним та важчим для злому.

WPA передбачає використання наступних методів аутентифікації:

- аутентифікація за допомогою попередньо встановленого ключа WPA-PSK (Pre-Shared Key) (Enterprise Autentification);
- аутентифікація за допомогою RADIUS-сервера (Remote Access Dial-in User Service).

Аутентифікація за допомогою попередньо встановленого ключа (Pre-Shared Key)

Для організації аутентифікації за допомогою попередньо встановленого ключа, точка доступу і клієнт повинні використовувати загальний ключ або кодове слово. Точка доступу відправляє клієнту випадковий рядок байтів. Клієнт приймає цій рядок, шифрує його, використовуючи ключ, і відправляє назад в точку доступу.

Точка доступу отримує зашифрований рядок і для розшифрування використовує свій ключ. Якщо розшифрований рядок, що був прийнятий від клієнта, збігається з вихідним рядком, що був відправлений клієнту, то клієнту дається дозвіл встановити з'єднання.

Недоліком аутентифікації за допомогою попередньо встановленого ключа WPA-PSK є те, що в цій технології виконується одностороння аутентифікація. PSK не передбачає перевірки пристроєм аутентичності точки доступу та не перевіряє справжність користувача, що намагається підключитися до точки доступу.

Аутентифікація на основі хешованного паролю

Велика частина ПЗ, що використовується в даний час, не використовує паролі в чистому вигляді, в місце цього використовуються їх

хеш-значення, одержувані за допомогою обчислення криптографічного хеш-функції [12].

Однонаправлені хеш-функції (далі хеш-функції) - це функції, які беруть на вході рядок різної довжини і перетворюють її у вихідний рядок фіксованої довжини, звану значенням хеш-функції (хеш-значення). Основною властивістю хеш-функцій є неможливість відновлення вихідної інформації за отриманим хеш-значенням [13].

Процедура проходження аутентифікації на основі хешованного паролю:

1. Користувач вводить пару username / password;

2. На стороні клієнта обчислюється хеш-значення password hash від введеного пароля password;

3. Пара username / password hash передаються сервера аутентифікації;

4. Сервер аутентифікації виробляє пошук облікового запису в базі даних і порівнює хеш пароля з збереженим значенням;

5. У разі збігу даних аутентифікація вважається успішною.

Аутентифікація за допомогою RADIUS-сервера

Аутентифікація за допомогою RADIUS-сервера [2] забезпечує взаємну аутентифікацію, а також аутентифікацію кожного конкретного користувача. Якщо на стороні клієнта встановлено програмне забезпечення EAP (Extensible Authentication Protocol), клієнт взаємодіє з внутрішнім сервером аутентифікації, таким, як служба віддаленої аутентифікації користувачів з комутованим доступом (RADIUS).

Цей внутрішній сервер працює незалежно від точки доступу та веде базу даних користувачів, які мають дозвіл на доступ в мережу. При застосуванні EAP користувач повинен пред'явити ім'я і пароль, що потім перевіряються по базі даних сервера RADIUS. Якщо пред'явлені облікові

дані є допустимими, користувач розглядається як той, що пройшов аутентифікацію (рис. 1.8).

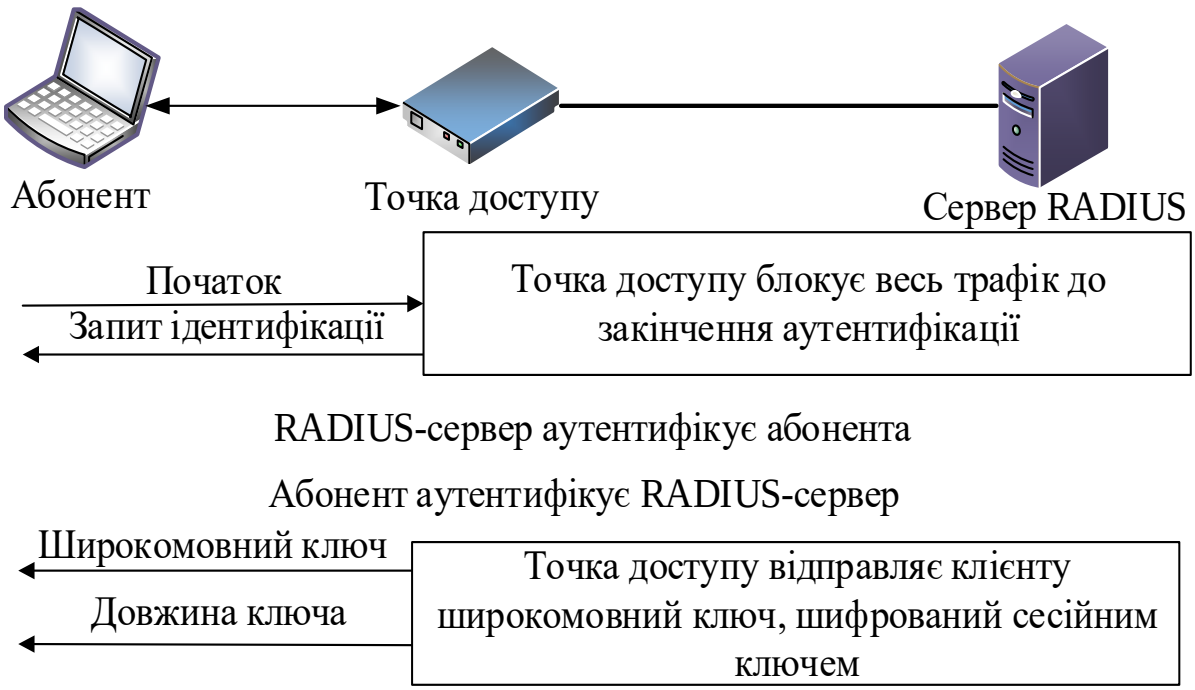


Рис. 1.8 - Аутентифікація за допомогою RADIUS-сервера

Аутентифікація з використанням MAC-адрес

Аутентифікація з використанням MAC-адрес не специфікована стандартом 802.11.x. але забезпечується багатьма виробниками. У ході аутентифікації з використанням MAC-адрес перевіряється відповідність MAC-адреси клієнта з локально сконфігурованого списку дозволених адрес або списку, що зберігається на зовнішньому сервері (рис. 1.9).

Аутентифікація з використанням MAC-адрес підсилює дію відкритої аутентифікації і аутентифікації з спільно використовуваних ключем, забезпечуваними стандартом 802.11x , потенційно знижуючи тим самим імовірність того, що неавторизовані пристрої отримають доступ до мережі.

Рис. 1.9 - Процес аутентифікації з використанням MAC-адрес

Уразливість аутентифікації з використанням MAC-адрес

MAC-адреси пересилаються за допомогою незашифрованих фреймів стандарту 802.11x, як і обумовлено в специфікації цього стандарту. В результаті бездротові LAN, в яких застосовується аутентифікація використанням MAC-адрес, уразливі для атак, в ході яких зловмисник «підкопується» під аутентифікацію з використанням MAC-адрес шляхом імітації «законної» MAC-адреси. Імітація MAC-адреси можлива для мережевих карт стандарту 802.11x, які дозволяють замінювати універсально-призначуваний адресу (universally administered address, UAA) локально-призначуваним (locally administered address, LAA). Універсальна адреса - це MAC-адреса, жорстко закодована для мережевої карти виробником. Атакуючий може використовувати аналізатор протоколу для визначення дозволеного в BSS MAC-адреси та мережеву карту, яка допускає локальне призначення адреси, для імітації дозволеної MAC-адреси.

Аутентифікація за токенами

Цей тип аутентифікації найчастіше використовується при побудові розподілених систем Single Sign-On (SSO), де додаток (service provider (SP))

передає обов'язки аутентифікації користувачів сторонньому додатку (identity provider (IP)). Найпоширенішим прикладом даного способу є вхід в додаток через обліковий запис в соціальних мережах (Facebook, Twitter), або через поштові сервіси (Google.com).

Реалізація даного способу полягає в тому, що IP надає достовірні відомості про користувача в вигляді токена, а SP використовує цей токен для аутентифікації користувача. У загальному випадку процес виглядає наступним чином (Рис. 1.10):

- Користувач аутентифікується у IP додатку;
- Користувач просить IP надати йому токен для будь-якого SP;
- IP генерує токен і відправляє його користувачеві;
- Клієнт аутентифікується в SP використовуючи токен наданий IP.

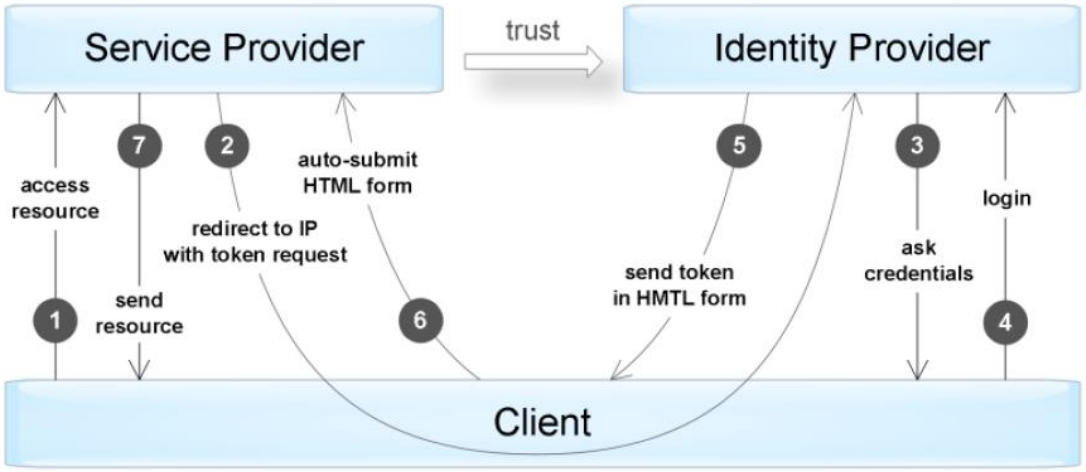


Рис. 1.10 - Аутентифікація з використовуванням токенов

Аутентифікація за QR-кодом

SQRL (Secure Quick Reliable Login) - протокол аутентифікації для безпечного входу на веб-сайт [4]. Для перевірки справжності, зазвичай, використовується QR-код. Користувач, при цьому, ідентифікується

анонімно замість того, щоб вводити логін і пароль. Загальну схему алгоритму можна представити таким чином :

- Користувач заходить на web-сторінку, яка підтримує SQRL протокол;
- За допомогою програми на мобільному телефоні (або плагіна для web-браузера) сканує представлений на сайті QR-код;
- Після сканування, на екрані телефону (або в web-браузері) відображається URL сайту, на який ви хочете увійти;
- Якщо відображений URL збігається з адресою сайту, користувач підтверджує вхід.

Детальніше SQRL можна описати таким чином [4]:

1. QR-код, представлений близько полів введення логіна і пароля, містить URL сервісу аутентифікації сайту. URL включає в себе надійно сгенероване випадкове число великої довжини таке, що кожна вистава сторінки входу містить різні QR-коди. (В криптографічних колах довге випадкове число так само називають "nonce");

2. SQRL-додаток для смартфона криптографически хешірует доменне ім'я сайту за допомогою майстер ключа користувача щоб створити унікальний для сайту пару публічний / приватний ключ;

3. Додаток криптографически підписує весь URL, що міститься в QR-коді, використовуючи специфічний для сайту приватний ключ. Так як URL включає в себе nonce, підпис є унікальною для сайту і QR-коду;

4. Додаток посилає безпечний HTTPS POST запит на URL кончини в QR-коді, який є сервісом аутентифікації сайту. POST запит надає специфічний для сайту публічний ключ і відповідну криптографічний підпис URL-а QR-коду;

5. Сервер аутентифікації отримує і підтверджує POST запит, повертаючи стандартний HTTP "200 OK" без будь-якого вмісту. SQRL додаток підтверджує успішне підписання користувачем QR-коду;

6. Сервер аутентифікації має URL, що містить nonce, який прийшов зі сторінки входу з програми користувача. Він також має криптографічний підпис цього URL, і специфічний для сайту публічний ключ користувача.

Сервіс використовує відкритий ключ для перевірки того, що підпис є дійсною для даного URL. Це підтверджує що користувач, який справив підпис, використовує секретний ключ, відповідний відкритого ключа. Після перевірки підпису, сервер аутентифікації розпізнає вже аутентифікованого користувача по його специфічному для сайту відкритому ключу.

Яндекс.Ключ

"Яндекс.Ключ" - це аутентифікатор, що генерує одноразові паролі, за допомогою яких здійснюється вхід на Яндекс, Facebook, Google, GitHub, Dropbox і інші сервіси, що підтримують двухфакторну аутентифікацію (2FA) [7]. З основних характеристик даного продукту можна виділити:

- Для використання цього додатку необхідно створення чотиризначного PIN-коду. Можливість змінити PIN-код відсутній. У ситуації, коли користувач забув PIN-код, відновити доступ до аккаунту можна тільки за допомогою служби технічної підтримки;
- Додавання різних сервісів в додаток відбувається вручну - републікуючи дані сайту з сервісу, або автоматично - зчитую QR-код;
- Даний аутентифікатор не вимагає підключення до інтернету, і не використовує SMS;
- Даний продукт вміє створювати шестизначні і восьмизначні паролі - в залежності від вимог сервісу. Також підтримуються різні періоди поновлення одноразових паролів.

Інтерфейс програми, що відображає введення PIN-коду, вибір сервісу для авторизації, і сам OTP, представлений на рисунку 2.11.

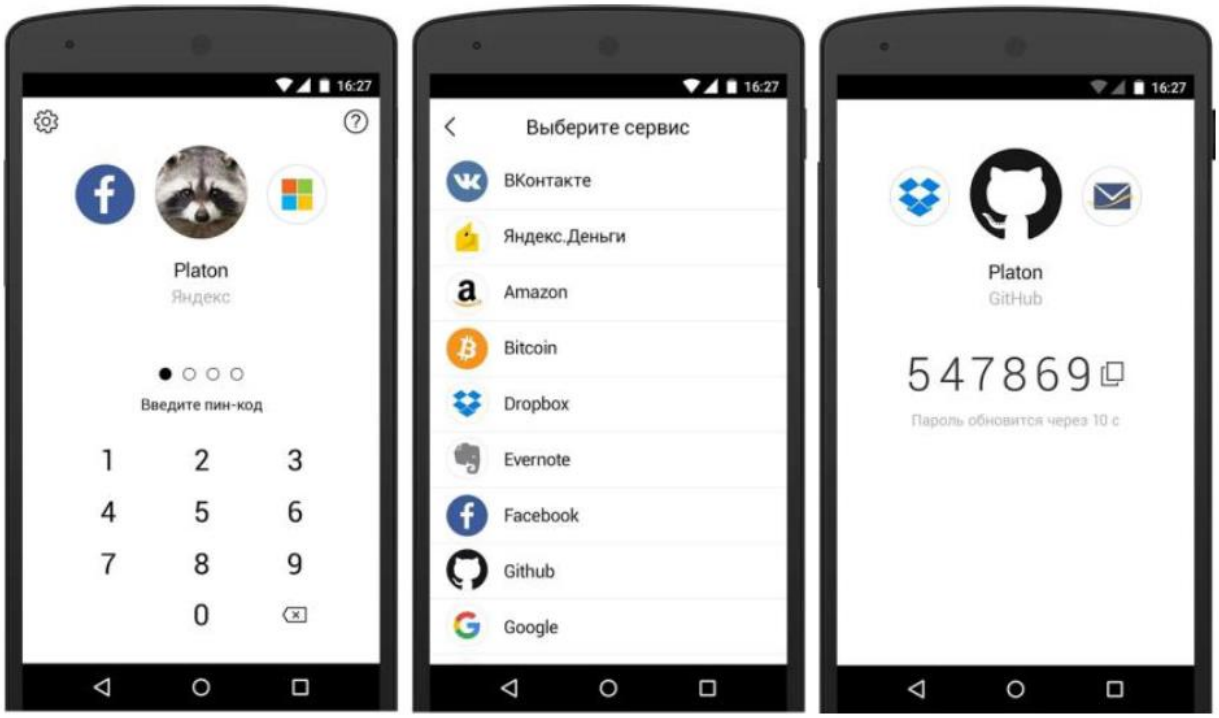


Рис. 1.11 -Інтерфейс аутентифікатору «Яндекс.Ключ»

Steam Guard

Steam Guard - це одна з функцій мобільного додатка Steam, для посилення захисту облікового запису [6].

З основних характеристик даного продукту можна виділити:

- Вхід до цього додатка здійснюється за коштами введення логіна і пароля від основного аккаунту, після цього з'являється можливість активувати функцію 2FA засновану на генерації OTP;
- Після активації 2FA, кожен вхід в аккаунт буде вимагати введення одноразового пароля;
- Є можливість відновлення аккаунту при втраті телефону, за допомогою коду відновлення, що надається при активації функції Steam Guard;

- Генерація OTP відбувається раз в 30 секунд без можливості зміни даного інтервалу;
- Не потрібне підключення до мережі;
- Програма є не тільки аутентифікатором, а так же мобільним додатком, що дозволяє використовувати базові функції Steam.

Інтерфейс програми, що відображає різні стани додатку представлений на рисунку 1.12.

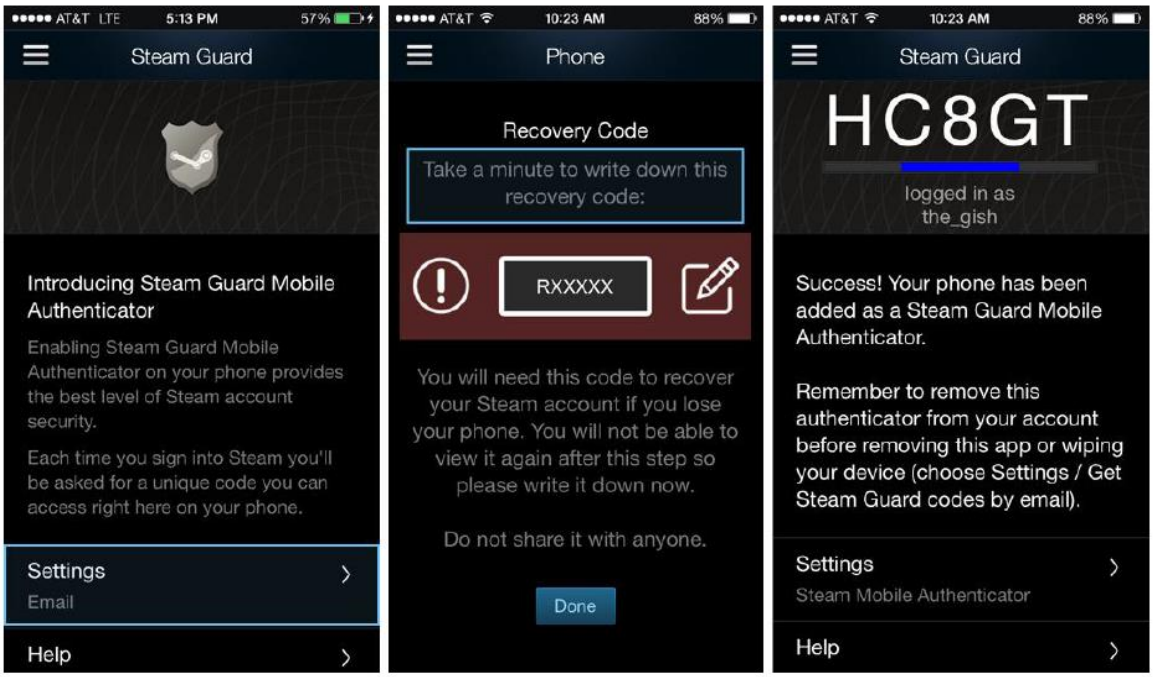


Рис. 1.12 - Інтерфейс аутентифікатору Steam Guard

"Battle.net" Authenticator

Аутентифікатор від компанії Blizzard дозволяює захистити обліковий запис на основі 2FA аутентифікації за коштами OTP [7]. З основних функцій програми можна виділити наступні:

- Є два типи кодів - 6 або 8-значні;
- Є функція запам'ятовування комп'ютера, що дозволяє не вводити код кожного разу при вході з одного і того ж пристрою;
- Є функція обмеження дії введеного коду для певного пристрою;

- Доступна можливість запрашіванія коду при кожному вході в акаунт;
- Необхідно підключення до інтернету і синхронізація часу;
- Є можливість відновлення доступу.

Інтерфейс програми представлений на рисунку 1.13.

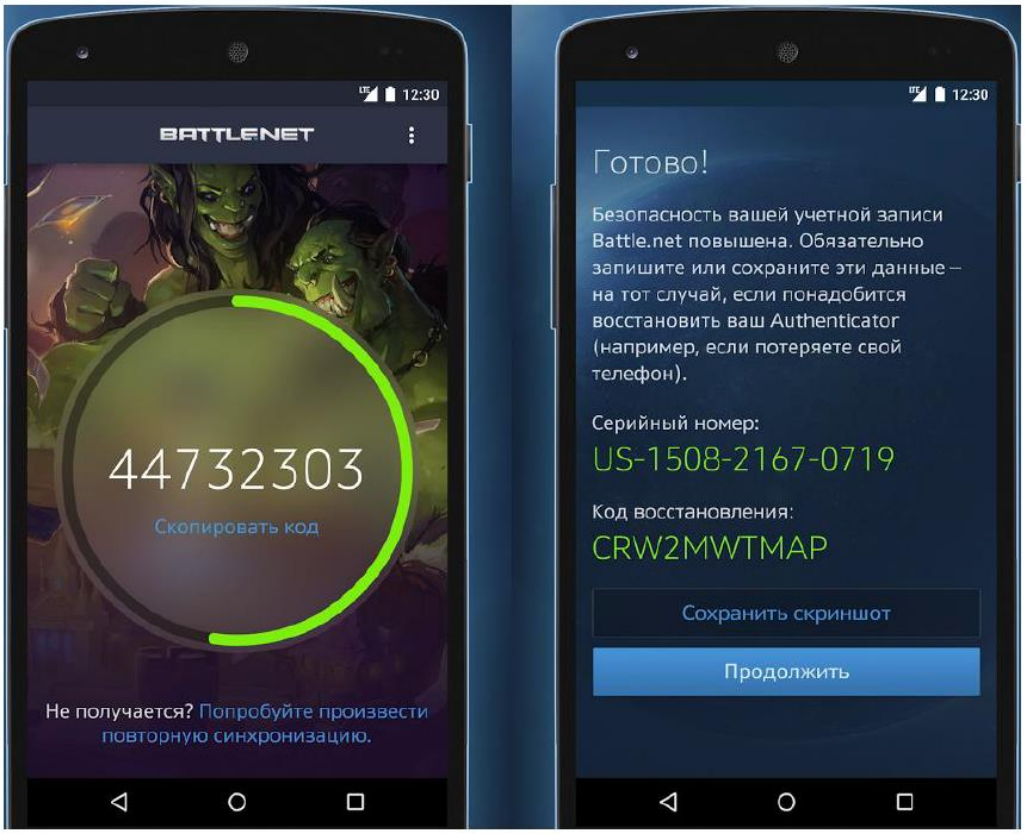


Рис. 1.12 - Інтерфейс аутентифікатору Battle.Net

Google Authenticator

Додаток Google Authenticator також засновано на генерації одноразових паролів для здійснення 2FA. Користувачем пропонується включити функцію двофакторної аутентифікації, для посилення захисту облікового запису, використовуючи для цього різні методи, як відправка SMS, або аутентифікація за допомогою розглянутого додатки [8].

З основних характеристик додатка можна виділити наступні:

- Генерація паролів без підключення до інтернету;

- Додавання декількох акаунтів на один пристрій аутентифікації;
- Наявність резервного методу аутентифікації за коштами списку одноразових паролів, роздрукованого на папері;
- Відсутність автоматизованого способу відновлення, при втраті пристрою;
- Одноразовий пароль оновлюється раз в 30 секунд.

Інтерфейс програми Google Authenticator представлений на малюнку 1.14.

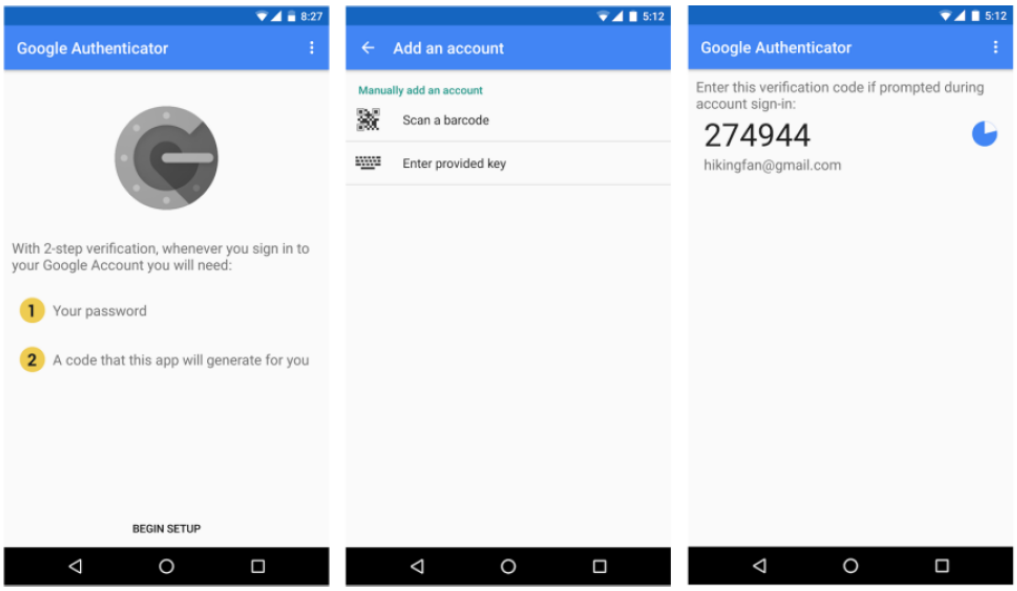


Рис. 1.14 -Інтерфейс інтерфейсу Google Authenticator

Огляд зарубіжних рівнів вимог до аутентифікації

У США розвиток рекомендацій, технічних вимог і стандартів на поділ за рівнями строгості аутентифікації має багату історію [8]. Основним, на даний момент, документом, що надає найбільш повну інформацію по аутентифікації і авторизації, є Electronic Authentication Guideline [9]. В даному документі є чотири рівні гарантії аутентифікації, засновані на аналізі ризиків помилок аутентифікації і можливих атак. Наведемо перелік основних загроз:

1. Реєстрація:

- «маскарад» - імітація конкретного користувача;
- 2) заперечення реєстрації.

2. Токени (аутентифікатор):
   - програмні і фізичні ключові носії можуть бути вкрадені або дубльовані;
   - відоме (Пароль, PIN-код) може бути розкрито зловмисником;
   - 3) володіє (образ сітківки, відбиток пальця) може бути скопійовано.
3. Протоколи аутентифікації:
   - підслуховування;
   - імітація (користувача, перевіряє / довіряє боку);
   - перехоплення сеансу аутентифицированного користувача (звернення від імені користувача до довіряє стороні з метою отримання конфіденційної інформації або введення неправдивої інформації);
   - звернення від імені довіряє боку до перевіряє стороні з метою отримання конфіденційної інформації або введення неправдивої інформації.
4. Інші загрози:
   - випадкові і / або навмисні помилки при виданні Credentials, зв'язуванні, делегування прав, створення облікових записів;
   - шкідливе ПО, спрямоване на компрометацію токенов (аутентифікатор);
   - вторгнення в системи користувачів, CSP або перевіряючих сторін з метою отримання цифрових посвідчень або токенів;
   - загрози компрометації токенов з боку інсайдерів;
   - соціальний інжиніринг з метою розкриття користувачем даних, підглядання;

- атаки, при яких обманутий заявник використовує небезпечний протокол, думаючи, що використовує безпечний, або сам долає засоби захисту (наприклад, приймаючи сертифікати серверів, які не пройшли перевірку);
- явна відмова користувачів, свідомо котрі скомпрометували свої маркери.

На основі проведеного аналізу було складено такі рівні гарантії аутентифікації:

- Перший рівень

  Не містить вимог до підтвердження справжності, але механізм аутентифікації надає деяку частку впевненості в тому, що заявник, який звертається до транзакції або даними, той, за кого себе видає. Аутентифікація визнається успішною, якщо заявник надає по протоколу безпечної аутентифікації доказ володіння аутентифікатором. Паролі або секрети не передаються по мережі у відкритому вигляді. Однак цей рівень не вимагає застосування криптографічних методів захисту. У багатьох випадках зловмисник, що володіє доступом до каналу зв'язку, має можливість відновити пароль, використовуючи атаку зі словником.

- Другий рівень

  Передбачає використання однофакторной аутентифікації в віддаленої мережі. Вводяться вимоги до підтвердження справжності. Аутентифікаційні секрети тривалого зберігання не довіряються жодної зі сторін, за винятком заявника, а перевіряючі сторони підкоряються постачальнику служби електронних посвідчень (Credentials Service Provider, CSP). (Однак CSP може надавати незалежним перевіряючим сторонам сеансу (тимчасові) загальні секрети.) Обов'язкове застосування дозволених криптографічних методів. Підтвердження справжності заявників, що випускаються в

результаті їх успішної аутентифікації, автентифіковані криптографически (дозволеними методами) або виходять безпосередньо від довіреної сторони щодо безпечного протоколу аутентифікації.

- Третій рівень

  Надає многофакторную (не менше двох) аутентифікацію в віддаленої мережі. Процедури підтвердження справжності вимагають перевірки ідентифікують матеріалів і інформації. Аутентифікація заснована на доказі володіння ключем або одноразовим паролем за криптографічним протоколом, потрібна наявність механізмів забезпечення строгості криптографії, що захищають первинні аутентифікатор (секретний ключ, закритий ключ або одноразовий пароль) від компрометації методами прослуховування, відтворення, онлайн-вгадування, імітації перевіряє боку і атаки «людина посередині ».

  Можуть використовуватися три види аутентифікатор: «програмні» криптографічні аутентифікатор, «апаратні» криптографічні аутентифікатор і апаратні генератори одноразових паролів. Аутентифікаційні секрети тривалого зберігання не довіряються жодної зі сторін, за винятком заявника, а перевіряючі сторони підкоряються CSP (Однак CSP може надавати незалежним перевіряючим сторонам сеансу (тимчасові) загальні секрети.) Для всіх операцій застосовуються легітимні криптографічні методи.

  Підтвердження справжності заявників, що випускаються в результаті їх успішної аутентифікації, автентифіковані криптографически або виходять безпосередньо від довіреної сторони щодо безпечного протоколу аутентифікації.

- Четвертий рівень

Призначений для забезпечення найстрогішої аутентифікації на основі докази володіння закритим ключем за криптографічним протоколом. Рівень 4 аналогічний рівню 3, за винятком того, що на ньому допускається використання тільки «апаратних» криптографічних аутентифікатор, посилені вимоги FIPS 140-2 до оцінки криптографічних модулів, і потрібно, щоб в подальшому справжність переданих конфіденційних даних підтверджувалася з використанням ключа, прив'язаного до процесу аутентифікації.

Аутентифікатор повинен бути апаратним криптографічним модулем, які мають сертифікат відповідності FIPS 140-2 рівня 2 або вище із забезпеченням фізичної безпеки на рівні не нижче FIPS 140-2 рівня 3. Потрібно сувора криптографічна іаутентифікація усіх боків і при всякій передачі конфіденційних даних між сторонами. Можуть використовуватися як симетричні, так і асиметричні криптографічні алгоритми. Аутентифікація вимагає підтвердження заявником володіння аутентифікатором з безпечного протоколу аутентифікації.

Повинно запобігати атаки прослуховування, відтворення, онлайн вгадування, імітації перевіряє боку і «людина посередині».

При використанні аутентифікаційних секретів тривалого зберігання вони не довіряються жодної зі сторін, за винятком заявника, а перевіряючі сторони підкоряються CSP. (Однак CSP може надавати незалежним перевіряючим сторонам сеансу (тимчасові) загальні секрети.) Для всіх операцій використовуються стійкі, схвалені криптографічні методи. При будь-якої передачі конфіденційної інформації здійснюється криптографічний аутентифікація з використанням ключів, прив'язаних до процесу аутентифікації.

2. РОЗРОБКА СПОСОБУ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ НА ОСНОВІ ОЦІНКИ ПАРАМЕТРІВ КАНАЛУ ЗВ'ЯЗКУ

2.1. Опис методу аутентифікації на фізичному рівні взаємодії

Так як бездротові пристрої широко поширені, вони стають більш вразливими до різних атак. Пристрої, які працюють в бездротової середовищі, мають низьку ціну, тому вони легкодоступні для потенційних зловмисників. Також, бездротові мережі відкриті для вторгнення ззовні і без необхідності фізичного з'єднання і, як наслідок, методи, які могли б забезпечити високий рівень безпеки в провідній мережі виявилися неефективними.

Однак звичайні криптографічні механізми забезпечення безпеки мають важливе значення для безпеки бездротових мереж, ці методи не використовують унікальні властивості бездротової мережі для усунення

загроз безпеки. Фізичні властивості бездротового середовища є потужним джерелом і можуть використовуватися для доповнення і розширення традиційних механізмів безпеки.

Використання унікального каналу між двома точками бездротової мережі, необхідно для того, щоб встановити нові форми аутентифікації, які включають інформацію, доступну на фізичному рівні. Замість того щоб покладатися тільки на криптографічні механізми вищого рівня, бездротові пристрої можуть аутентифицировать себе на основі їх здатності продукувати відповідний сигнал.

З метою підвищення безпеки бездротової мережі доцільно для аутентифікації використовувати оцінку місця розташування. Місцезнаходження користувача є важливою ознакою, який може бути використаний для аутентифікації користувача.

Аутентифікація на основі розташування є досить новим напрямком в інформаційній безпеці. Розвиток цього напрямку в даний час має особливе місце для мобільних пристроїв в галузі бездротових мереж. Така аутентифікація не вимагає участі людини, на відміну від методів аутентифікації зазначених вище.

Можливість приймача визначати, коли передавач змінив своє місце розташування, має важливе значення для збереження енергії в бездротових мережах, для фізичної безпеки об'єктів, а також для забезпечення безпеки бездротової мережі по виявленню атак реплікації.

Місцезнаходження має вирішальне значення для забезпечення безпеки, і щоб мати можливість зосередити ресурси (наприклад, камер безпеки, персонал) на рухомих об'єктах. Оцінка місця розташування повинна бути зроблена в енергетично ефективному режимі, особливо для мереж з невеликими батареями, які змогли б працювати протягом багатьох років. Енергія, необхідна для оцінки місця розташування повинна бути витрачена при русі об'єкта. Однак в таких системах слід

уникати повторного оцінювання розташування до тих пір, поки місце розташування не зміниться. Тоді, для енергетичної ефективності буде легше визначити, змінилося місце розташування чи ні.

2.2. Принцип надійного визначення місцезнаходження з використанням бази даних поточних вимірювань

Розглянемо надійний алгоритм визначення зміни місця розташування об'єктів, який використовує канальний рівень взаємодії між передавачем і приймачем, заснований на базі даних поточних вимірювань.

База даних вимірювань - це сума значень параметрів багатопроменевого поширення від передавача до приймача, де кожен об'єкт має власну амплітуду, фазу і тимчасову затримку. Значення бази даних змінюється, коли передавач або приймач змінює своє положення.

Наприклад, було розглянуто карту вузлів (передавачів) і приймачів на рисунку 2.1, в якому приймач виступає в якості сервера аутентифікації, а вузли (передавачі) - користувачами.

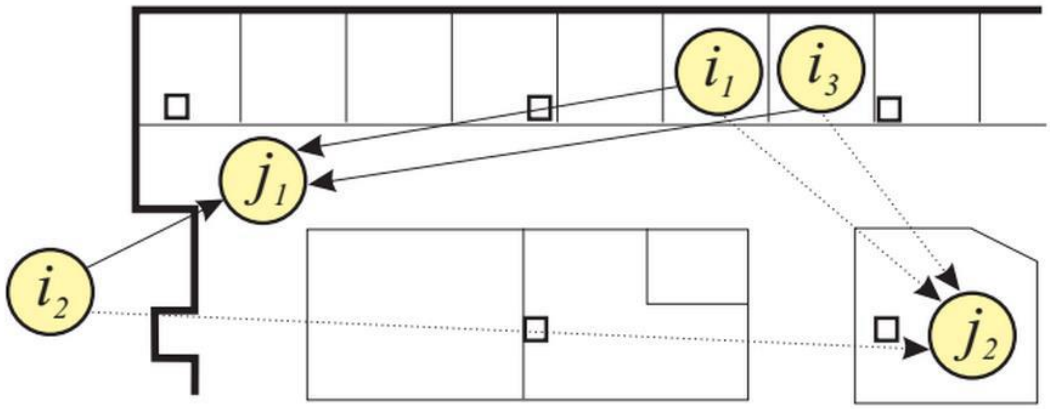


Рисунок 2.1 - Карта вузлів

Приймачі j_1 та j_2 отримують пакети від передавачів i_1, i_2, i_3. Порівнюючи значення прийнятого сигналу за значеннями бази даних, можна відрізнити передавачі по їх розташуванню.

Визначимо зв'язок між вузлами в i_1 та j_1. Приймач вузла j_1 може вимірювати і записувати виміряне значення в базу даних. Коли передатчік i_1 переміщається в місце, наприклад, відповідне вузлу i_3, то вузол j_1 може відрізнити нове значення від раніше записаного значення, і він фіксує, що вузол i_1 змінив своє місце розташування .

Якщо порушник i_2 видає себе за легального користувача, то його передача в вузол j_1 буде виявлена і попереджена.

Інші приймачі можуть також брати участь в процесі виявлення порушника для більш високої надійності і стійкості виявлення зміни послідовності. На відміну від існуючих методів, методи виявлення зміни місця розташування, що використовують бази даних, не вимагають тривалої роботи.

Після прийому чергового пакета, приймач може виявити, що передавач перемістився з моменту його минулого передачі.

Було проведено детальний аналіз цього методу, визначено базу даних вихідних розташування й запропоновано алгоритм аутентифікації об'єктів мережі на основі аналізу сигналів. Крім того, розглянуто, алгоритм спільного використання декількох приймачів для досягнення ще більш високої надійності.

Даний спосіб має вирішувати задачу виявлення нелегального користувача в мережі або якщо якийсь користувач видає себе за іншого.

2.3. Алгоритм аутентифікації об'єктів мережі на основі аналізу параметрів сигналів на фізичному рівні

Алгоритм аутентифікації базується на відстежуванні змін характеристики каналу зв'язку для кожної пари передавач-приймач.

Для оцінки такої характеристики пропонується використовувати імпульсну характеристику каналу смуги частот, яка зайнята сигналом,

що передається. Нехай така оцінка буде вважатися радіовідбитком каналу. Ідею алгоритму можна викласти як наступну послідовність дій:

- Створюється база даних поточних вимірювань для «легальних» користувачів, так звана історія вимірювань, що складається з історій вимірювань радіовідбитка каналу між приймачем (*j*) і кожним з передавачів (*i*) для *N-1* вимірів. Усі вони записуються у вигляді матриці.

$$H_{i,j} = \left\{ h_{i,j}^{(n)} \right\}_{n=1}^{N-1} \qquad (1)\ [2].$$

- Для врахування впливу випадкових тимчасових характеристик каналу і шуму обчислюється величина $\sigma_{i,j}$ - середня відстань між *N-1* виміром в $H_{i,j}$.

$$\sigma_{i,j} = \frac{1}{(N-1)(N-2)} \sum_{g \in H_{i,j}} \sum_{h \in H_{i,j} \setminus g} \|h - g\| \qquad (2)\ [3],$$

де || *h* - *g* || - різниця значень параметрів між парами вузлів в поточному вимірі, *g* – поточне значення вузла, *h* – поточне значення інших вузлів, $H_{i,j}$ – поточне вимірювання, *i* – вузел, *g* – приймач, *N* – номер виміру [4].

- Проводиться черговий вимір радіовідбитку каналу $h_{i,j}^{(N)}$.
- Розрахунок мінімальної евклідової відстані між поточним виміром $h_{i,j}^{(N)}$ та історією вимірювань $H_{i,j}$.

$$d_{i,j} = \frac{1}{\sigma_{i,j}} \min_{h \in H_{i,j}} \left\| h - h^{(N)} \right\| \quad (3)\ [5],$$

де h – поточне значення інших вузлів, $H_{i,j}$ – поточне вимірювання, i – вузел, g – приймач, N – номер виміру, $\sigma_{i,j}$ - середня відстань між N-1 виміром в $H_{i,j}$.

- Перебір усіх значень, $d_{i,j}$. Порівнюємо значення, $d_{i,j}$ з граничним значенням γ, де γ> 0. Якщо відстань, $d_{i,j}$ > γ, приймається рішення про те, що різниця між виміряним значенням «радіовідбитка» каналу і історією обумовлена тим, що виміряне значення належить іншому каналу зв'язку. Фіксується факт невірної аутентифікації.

- Якщо відстань, $d_{i,j}$ < γ, то робимо висновок, що положення об'єкта підтверджується (не змінилося) і нове значення $h_{i,j}^{(N)}$ включається в базу даних $H_{i,j}$, а найстаріше значення видаляється.

Далі визначається ймовірність правильного виявлення того, що положення передавача не змінилося і ймовірність хибної тривоги. Нехай i - дозволене положення передавача, а i '- передавач-порушник. Необхідно визначити чи дійсно і ' не є об'єктом і. Для цього необхідно порівняти $d_{i\text{-}i',j}$ з $d_{i,j}^{(N)}$.

При цьому можливі такі припущення:

- H0: $d_{i,j} = d_{i,j}^{(N)}$, тобто об'єкт істинний;
- H1: $d_{i,j} = d_{i\text{-}i',j}$, тобто об'єкт помилковий.

Для цих припущенн можна ввести ймовірності:

- P_{FA} - ймовірність помилкової тривоги;
- P_D - ймовірність виявлення.

Оскільки випадкова величина $d_{i,j}$ схильна до впливу величезного числа випадкових перешкод, то вона має гауссовський розподіл. Для цих величин справедливо наступне:

$$P_{FA} = \sqrt{\frac{1}{2\pi\sigma_{i,j}^2}} \int_{\gamma}^{\infty} e^{-\frac{1}{2\sigma_{i,j}^2}\left(x-d_{i,j}^{N}\right)^2} dx, \quad (4) [6],$$

$$P_D = \frac{1}{\sqrt{2\pi\sigma_{i,j}^{\ 2}}} \int_{\gamma}^{\infty} e^{-\frac{1}{2\sigma_{i,j}^{\ 2}}\left(x-d_{i,j}\right)^2} dx, \quad (5) [2],$$

де γ - поріг прийняття рішення.

Зазвичай $P_D \approx 1$ [3], тому можна використовувати ймовірність $P_M = 1-P_D$ - ймовірність пропуску.

Блок-схема алгоритму аутентифікації зображено на рисунку 2.2.

3. ДОСЛІДЖЕННЯ АЛГОРИТМУ АУТЕНТИФІКАЦІЇ ОБ'ЄКТІВ НА ОСНОВІ АНАЛІЗУ ПАРАМЕТРІВ СИГНАЛІВ

3.1. Моделювання алгоритму аутентифікації об'єктів мережі на основі аналізу параметрів сигналів

Моделювання алгоритму проводиться в середовищі Matlab. Розглянемо офіс в сучасній будівлі, в якій розташовані наші вузли (користувачі). В даній мережі, що складається з 9 вузлів, необхідно

розробити спосіб, що дозволяє вузлам аутентифікувати один одного на основі параметрів сигналу.

Припустимо, приймачем j є вузол 11, який буде аутентифікувати об'єкти, а вузли 1, 2, 3, 4, 5, 6, 7, 8, 9 - передавачами (користувачі). У мережі, що було розроблено, сервером аутентифікації є точка доступу 11 (рисунок 3.1).

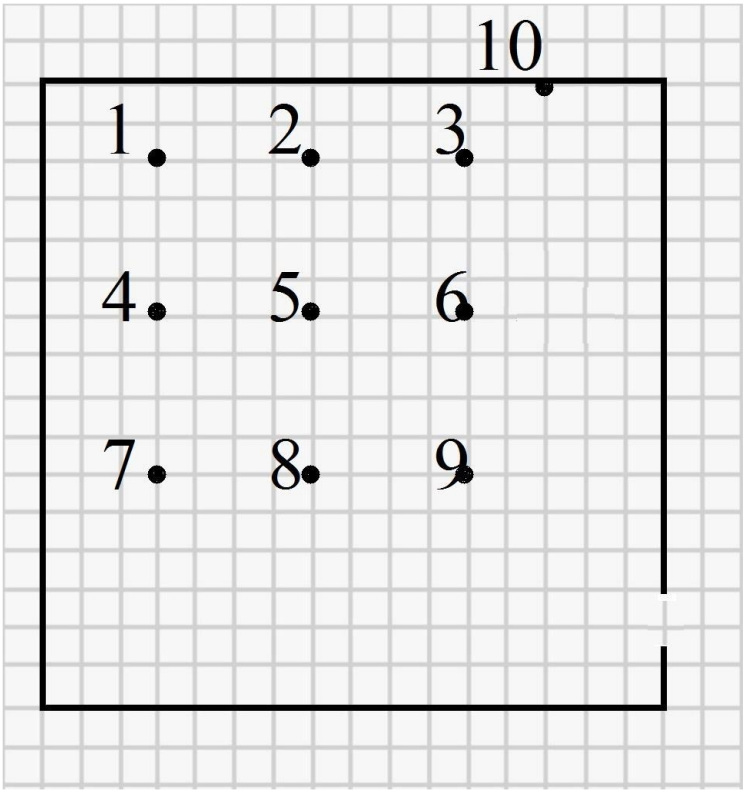


Рис.3.1 - Карта розташування вузлів в мережі

Досліджуваним сигналом є OFDM-сигнал (Orthogonal frequency-division multiplexing - мультиплексування з ортогональним частотним поділом каналів, є цифровою схемою модуляції, яка використовує велику кількість близько розташованих ортогональних піднесучих.

Кожна піднесуща модулюється за звичайною схемою модуляції (наприклад, квадратурная амплітудна модуляція) на низькій символьної швидкості, зберігаючи загальну швидкість передачі даних, як і у звичайних схемі модуляції однієї несучої в тій же смузі пропускання.

На практиці сигнали OFDM виходять застосуванням зворотного ШПФ (Швидке перетворення Фур'є)) [3] з наступними параметрами:

- розмірність БПФ: 128;
- величина захисного інтервалу по частоті: зліва 8, справа 7;
- центральна піднесуща має нульову амплітуду;
- спосіб маніпуляції на інформаційних піднесущих: ФМ-2;
- спосіб маніпуляції на пілотних піднесущих: ФМ-2;
- тривалість циклічного префіксу: 16 відліків (1/8 тривалість
- OFDM-символу);
- частота дискретизації: 40 МГц.
- для кожного вузла генерується своя послідовність на всі генеруються OFDM-символи, що генеруються.

Складемо історію бази даних поточних вимірювань параметрів вузлів1, 2, 3, 4, 5, 6, 7, 8, 9 з 5 вимірів, яку веде вузол 11. Поточні вимірюваннябули отримані в такий спосіб:

- сформувалися OFDM-сигнали;
- сформовані OFDM-сигнали було пропущено через створений

канал;

- для запису даних запишемо її у вигляді матриці 3 х 3, де кожен

елемент матриці буде позначати вузол: $H_{i,j}(N) = h_{i,j}$.

База даних поточних вимірювань для 5 вимірів:

$$H_{i,j}^{(1)} = \begin{bmatrix} 45.900 & 48.003 & 43.124 \\ 44.408 & 44.632 & 45.514 \\ 45.328 & 47.685 & 42.997 \end{bmatrix}$$

$$H_{i,j}^{(2)} = \begin{bmatrix} 44.934 & 46.735 & 45.275 \\ 44.199 & 45.015 & 48.147 \\ 47.036 & 45.892 & 48.785 \end{bmatrix}$$

$$H_{i,j}^{(3)} = \begin{bmatrix} 45.356 & 45.302 & 48.496 \\ 42.929 & 45.086 & 45.102 \\ 46.093 & 47.115 & 42.401 \end{bmatrix}$$

$$H_{i,j}^{(4)} = \begin{bmatrix} 44.951 & 42.788 & 47.082 \\ 45.664 & 46.187 & 44.396 \\ 42.462 & 44.788 & 48.656 \end{bmatrix}$$

$$H_{i,j}^{(5)} = \begin{bmatrix} 45.022 & 44.978 & 45.894 \\ 41.974 & 44.130 & 47.788 \\ 45.180 & 42.648 & 48.181 \end{bmatrix}$$

Знайдемо «відстані» між поточним станом і базою даних за формулою (3). Для цього переберемо все значення виразу | h – g | за формулою (2), щоб знайти середню «відстань». | h – g | - це різниця значень параметрів між парами вузлів в поточному вимірі, де g - це поточне значення вузла, а h- поточні значення інших вузлів, в даному випадку, з матриці 3 х 3, у нас вийде 36 пар.

Різниця | h – g | для першого виміру.

$$||h-g|| = \begin{vmatrix} 0 & 2.103 & 2.775 & 1.491 & 1.267 & 0.385 & 0.571 & 1.785 & 2.902 \\ 2.103 & 0 & 4.879 & 3.595 & 3.595 & 2.489 & 2.674 & 0.318 & 5.006 \\ 2.775 & 4.879 & 0 & 1.28 & 1.508 & 2.390 & 2.204 & 4.561 & 0.127 \\ 1.491 & 3.595 & 1.28 & 0 & 0.224 & 1.106 & 0.920 & 3.277 & 1.410 \\ 1.267 & 3.595 & 1.508 & 0.224 & 0 & 0.882 & 0.696 & 3.052 & 1.635 \\ 0.385 & 2.489 & 2.390 & 1.106 & 0.882 & 0 & 0.185 & 2.170 & 2.517 \\ 0.571 & 2.674 & 2.204 & 0.920 & 0.696 & 0.185 & 0 & 2.356 & 2.331 \\ 1.785 & 0.318 & 4.561 & 3.277 & 3.052 & 2.170 & 2.356 & 0 & 4.688 \\ 2.902 & 5.006 & 0.127 & 1.410 & 1.635 & 2.517 & 2.331 & 4.688 & 0 \end{vmatrix}$$

Різниця | h – g | для другого виміру.

$$||h-g|| = \begin{vmatrix} 0.000 & 1.802 & 0.342 & 0.734 & 0.081 & 3.213 & 2.102 & 0.958 & 3.852 \\ 1.802 & 0.000 & 1.460 & 2.536 & 1.721 & 1.411 & 0.301 & 0.843 & 2.050 \\ 0.342 & 1.460 & 0.000 & 1.076 & 0.261 & 2.871 & 1.761 & 0.617 & 3.510 \\ 0.734 & 2.536 & 1.076 & 0.000 & 0.815 & 3.947 & 2.837 & 1.693 & 4.586 \\ 0.081 & 1.721 & 0.261 & 0.815 & 0.000 & 3.132 & 2.021 & 0.877 & 3.771 \\ 3.213 & 1.411 & 2.871 & 3.947 & 3.132 & 0.000 & 1.110 & 2.255 & 0.639 \\ 2.102 & 0.301 & 1.761 & 2.837 & 2.021 & 1.110 & 0.000 & 1.144 & 1.749 \\ 0.958 & 0.843 & 0.617 & 1.693 & 0.877 & 2.255 & 1.144 & 0.000 & 2.893 \\ 3.852 & 2.050 & 3.510 & 4.586 & 3.771 & 0.639 & 1.749 & 2.893 & 0.000 \end{vmatrix}$$

Різниця | h – g | для третього виміру.

$$\begin{vmatrix} 0.000 & 0.054 & 3.140 & 2.428 & 0.271 & 0.254 & 0.737 & 1.759 & 2.955 \\ 0.054 & 0.000 & 3.195 & 2.373 & 0.216 & 0.200 & 0.791 & 1.813 & 2.901 \\ 3.140 & 3.195 & 0.000 & 5.568 & 3.411 & 3.395 & 2.404 & 1.381 & 6.096 \end{vmatrix}$$

$$||h-g|| = \begin{vmatrix} 2.428 & 2.373 & 5.568 & 0.000 & 2.157 & 2.173 & 3.164 & 4.187 & 0.528 \\ 0.271 & 0.216 & 3.411 & 2.157 & 0.000 & 0.016 & 1.007 & 2.030 & 2.685 \\ 0.254 & 0.200 & 3.395 & 2.173 & 0.016 & 0.000 & 0.991 & 2.013 & 2.701 \\ 0.737 & 0.791 & 2.404 & 3.164 & 1.007 & 0.991 & 0.000 & 1.023 & 3.692 \\ 1.759 & 1.813 & 1.381 & 4.187 & 2.030 & 2.013 & 1.023 & 0.000 & 4.714 \end{vmatrix}$$

Різниця | h – g | для четвертого виміру.

$$||h-g|| = \begin{vmatrix} 0.000 & 2.162 & 2.131 & 0.713 & 1.236 & 0.555 & 2.488 & 0.163 & 3.705 \\ 2.162 & 0.000 & 4.293 & 2.875 & 3.398 & 1.607 & 0.326 & 1.999 & 5.868 \\ 2.131 & 4.293 & 0.000 & 1.418 & 0.895 & 2.686 & 4.619 & 2.294 & 1.574 \\ 0.713 & 2.875 & 1.418 & 0.000 & 0.523 & 1.268 & 3.201 & 0.876 & 2.992 \\ 1.236 & 3.398 & 0.895 & 0.523 & 0.000 & 1.791 & 3.724 & 1.399 & 2.469 \\ 0.555 & 1.607 & 2.686 & 1.268 & 1.791 & 0.000 & 1.933 & 0.392 & 4.261 \\ 2.488 & 0.326 & 4.619 & 3.201 & 3.724 & 1.933 & 0.000 & 2.325 & 6.194 \\ 0.163 & 1.999 & 2.294 & 0.876 & 1.399 & 0.392 & 2.325 & 0.000 & 3.868 \\ 3.705 & 5.868 & 1.574 & 2.992 & 2.469 & 4.261 & 6.194 & 3.868 & 0.000 \end{vmatrix}$$

Запишемо значення різниці | h – g | у таблицю у відповідність парам вузлів.

Таблиця 3.1 - Різниця | h – g | для N–1 вимірів

Пари вузлів	Різниця |h – g| для вимірів:			
	1	2	3	4
12	2.215	1.913	0.165	2.157
13	2.887	0.453	3.251	2.103
14	1.504	0.845	2.539	0.619
15	1.378	0.192	0.382	1.189
16	0.496	3.324	0.365	0.778
17	0.682	2.213	0.848	2.518
18	1.896	0.999	1.865	0.115
19	2.914	3.963	2.998	3.689
23	4.990	1.571	3.215	4.280

24	3.607	2.647	2.484	2.925
25	3.482	1.832	0.327	3.499
26	2.590	1.522	0.300	1.570
27	2.786	0.412	0.802	0.328
28	0.429	0.954	1.830	2.100
29	5.118	2.161	2.945	5.979
34	1.395	1.187	5.601	1.529
35	1.619	0.372	3.504	0.903
36	2.499	2.982	3.403	2.797
37	2.315	1.872	2.200	4.720
38	4.662	0.728	1.505	2.305
39	0.238	3.621	5.998	1.685
45	0.335	0.926	2.230	0.634
46	1.218	3.997	2.279	1.379
47	0.955	2.948	3.178	3.312
48	3.388	1.717	4.289	1.987
49	1.522	4.697	0.607	3.018
56	0.993	3.243	0.015	1.802
57	0.758	2.132	0.998	3.835
58	3.164	0.988	2.100	1.401

59	1.746	3.882	2.798	2.570
67	0.297	1.221	0.880	2.044
68	2.282	2.366	2.001	0.404
69	2.629	0.745	2.670	4.372
78	2.468	1.255	1.020	2.436
79	2.443	1.855	3.709	6.206
89	4.799	2.905	4.718	3.979

Після того, як ми порахували різницю, обчислимо за формулою (2) середню різницю серед всіх значень в базі даних:

$$\sigma_{i,j} = \begin{vmatrix} 0.000 & 0.514 & 0.772 & 0.701 & 0.312 & 0.598 & 0.505 & 0.587 & 1.381 \\ 0.514 & 0.000 & 1.229 & 1.199 & 0.796 & 0.710 & 0.358 & 0.609 & 1.586 \\ 0.772 & 1.229 & 0.000 & 1.105 & 0.653 & 1.103 & 0.975 & 1.008 & 1.133 \\ 0.701 & 1.199 & 1.105 & 0.000 & 0.490 & 1.192 & 1.111 & 0.892 & 1.310 \\ 0.312 & 0.796 & 0.653 & 0.490 & 0.000 & 0.790 & 0.708 & 0.737 & 1.218 \\ 0.598 & 0.710 & 1.103 & 1.192 & 0.790 & 0.000 & 0.569 & 0.998 & 0.876 \\ 0.505 & 0.358 & 0.975 & 1.111 & 0.708 & 0.569 & 0.000 & 0.782 & 1.414 \\ 0.587 & 0.609 & 1.008 & 0.892 & 0.737 & 0.998 & 0.782 & 0.000 & 1.808 \\ 1.381 & 1.586 & 1.133 & 1.310 & 1.218 & 0.876 & 1.414 & 1.808 & 0.000 \end{vmatrix}$$

Так як дистанція у нас симетрична, то необхідно порахувати тільки половину || h - g ||, отже, середня відстань серед всіх значень в базі даних ми можемо записати в таблицю.

Таблиця 3.2 - Значення параметру $\sigma_{i,j}$ між вузлами

Пари вузлів	Значення параметру $\sigma_{i,j}$
12	0.563

13	0.688
14	0.840
15	0.572
16	1.141
17	0.820
18	0.645
19	1.383
23	0.683
24	0.449
25	0.595
26	0.944
27	0.537
28	0.430
29	0.950
34	0.435
35	0.620
36	1.273
37	0.547
38	0.862
39	0.891

45	0.671
46	0.948
47	0.356
48	0.688
49	0.600
56	0.681
57	0.916
58	0.924
59	1.186
67	1.166
68	0.989
69	0.936
78	0.661
79	0.767
89	0.930

- Було розраховано мінімальну відстань між поточним виміром каналу й історією вимірювань.
- Було перебрано усі значення d_{ij} та порівняно їх за граничним значенням γ. Якщо відстань $d_{ij} < \gamma$, то робимо висновки, що положення об’єкту не змінилося і, отже, наш об’єкт достовірний.

Таблиця 3.2 - Значення параметру $d_{i,j}$ між вузлами

Пари вузлів	Значення параметру $d_{i,j}$
12	3.122
13	0.929
14	8.359
15	2.530
16	1.889
17	0.677
18	1.149
19	0.752
23	3.519
24	23.778
25	0.563
26	3.998
27	1.270
28	1.362
29	1.275
34	17.911

35	0.134
36	1.005
37	2.285
38	1.231
39	0.855
45	0.692
46	1.611
47	1.115
48	0.337
49	0.222
56	4.314
57	0.638
58	0.765
59	0.848
67	0.520
68	0.783
69	1.194
78	0.132
79	0.491

89	0.950

3.2. Вибір порогового значення при різних можливостях помилкової тривоги

Розглянемо як залежать порогові значення γ від різних значень ймовірності помилкової тривоги для пари вузлів 1-2. Щоб знайти поріг, ми використовуємо критерій Неймана-Пірсона. Згідно даним критерієм вибирається таке правило виявлення, яке забезпечує мінімальну величину ймовірності пропуску сигналу (максимальну ймовірність правильного виявлення) за умови, що ймовірність помилкової тривоги не перевищує величини, що було задано.

Для того щоб знайти параметр γ, розглянемо формулу (7) і зробимо наступну заміну:

$$P_{FA} = \sqrt{\frac{1}{2\pi\sigma_{i,j}^2}} \int_{\gamma}^{\infty} e^{\frac{1}{2\sigma_{i,j}^2}\left(x - d_{i,j}^N\right)^2} dx \tag{7}$$

$$t = \frac{\left(x - d_{i,j}^N\right)}{\sigma_{i,j}} \tag{8}$$

$$P_{FA} = \sqrt{\frac{1}{2\pi}} \int_{\frac{\left(\gamma - d_{i,j}^N\right)}{\sigma_{i,j}}}^{\infty} e^{-\frac{t^2}{2}} dt \tag{9}$$

Тоді, користуючись таблицею ймовірностей Лапласа, можна знайти значення порогу γ.

Наприклад, для ймовірності $P_{FA} = 0.15$, при значеннях між вузлами 1-2: $d_{i,j} = 3.099$ та $\sigma_{i,j} = 0.452$, величина аргументу t дорівнює 0.39, тоді:

$$t = \frac{(\gamma - d_{i,j}^N)}{\sigma_{i,j}} = 0.39,$$

$$\gamma = 0.39\sigma_{i,j} + d_{i,j}^N,$$

$$\gamma = 3.38639$$

За допомогою підстановки порогових значень γ до формули (5) знаходиться ймовірність виявлення P_D за таблицею функції Лапласа. В таблиці 3.4. можна знайти деякі значення t й ймовірностей помилкових тривог P_{FA}.

Таблиця 3.4 - Залежність ймовірності помилкової тривоги від порогового значення

P_{FA}	t
0.001	0.01
0.01	0.03
0.03	0.08
0.05	0.13
0.07	0.18
0.09	0.23
0.1	0.26
0.12	0.31
0.15	0.39
0.17	0.44
0.2	0.53

0.23	0.62
0.25	0.68
0.3	0.85

3.5. Моделювання алгоритму аутентифікації об'єктів мережі на основі аналізу параметрів сигналів для декількох приймачів

Нехай, новий об’єкт *i’*, що є вузлом №11, буде намагатися довести приймачу №10, що він є легальним вузлом №6.

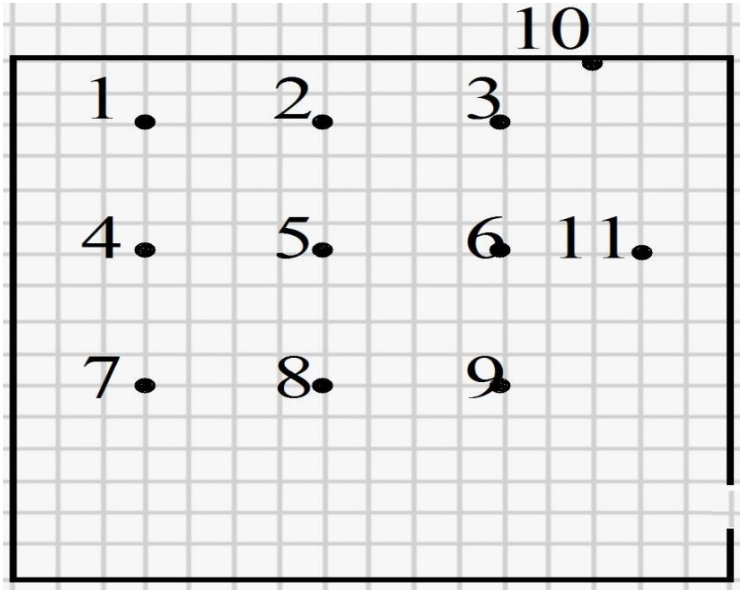


Рис.3.2 - Карта розташування пристроїв в мережі при появі порушника (вузел №11)

Одже, приймач додає нові значення вузла *i’* й обчислює для нього евклідову відстань між поточним виміром й історією.

У якості пари вузлів, для зрівняння евклідової відстані, виберемо вузел №3. Тобто, розглянуто пари вузлів №3-6 й №3-11.

Таблиця 3.5 - Параметри евклідової відстані для виявлення недостовірного користувача для пар вузлів №3-6 й №3-11

Пари вузлів	$d_{i,j}$

№3-6	0.603
№3-11	0.989

Також, обчислено поріг γ для P_{FA} = 0.25 й отримано, що $\gamma = 0.68$. Отже, $d_{i',j}$ = 0.941 більше за поріг, що було задано, отже, можна сказати, що даний об'єкт не є достовірним.

За умови, що $d_{i',j} < \gamma$, база даних останнього виміру було би змінено й значення історії вимірів було би оновлено.

Розраховано ймовірності для гіпотез, що були наведені. Задано різні значення P_{FA} й розглянуто як змінюється значення ймовірності виявлення в залежності від порогу.

Розраховано значення порогу для вузлів №3-6.

Відомо, що $\gamma = t\sigma_{i,j} + d_{i,j}^{N}$. За допомогою підстановки даного значення у формулу (5), було одержано:

$$P_D = \frac{1}{\sqrt{2\pi\sigma_{i,j}^{\,2}}} \int_{\gamma}^{\infty} e^{-\frac{1}{2\sigma_{i,j}^{\,2}}\left(x-d_{i',j}\right)^2} dx,$$

$$t = \frac{\left(x - d_{i',j}\right)}{\sigma_{i,j}},$$

$$P_D = \sqrt{\frac{1}{2\pi}} \int_{\frac{(\gamma - d_{i',j})}{\sigma_{i,j}}}^{\infty} e^{-\frac{t^2}{2}} dt.$$

Треба мати на увазі, що значення P_{FA} було вибрано в межах [0:0.3], так як ймовірність значення, що було дано вище, буде призводити до частих помилок виявлення.

Таблиця 3.6 - Значення ймовірностей P_{FA} й P_D

P_{FA}	P_D
0.001	0.632
0.01	0.703

0.03	0.759
0.05	0.778
0.07	0.795
0.09	0.812
0.1	0.823
0.12	0.833
0.15	0.865
0.17	0.881
0.2	0.815
0.23	0.62
0.25	0.931
0.3	0.985

У таблиці 3.6 представлено залежності P_{FA} від P_D, які було розраховано за умови різних γ за формулами. Ці ж залежності для наочності було представлено на рисунку 3.3.

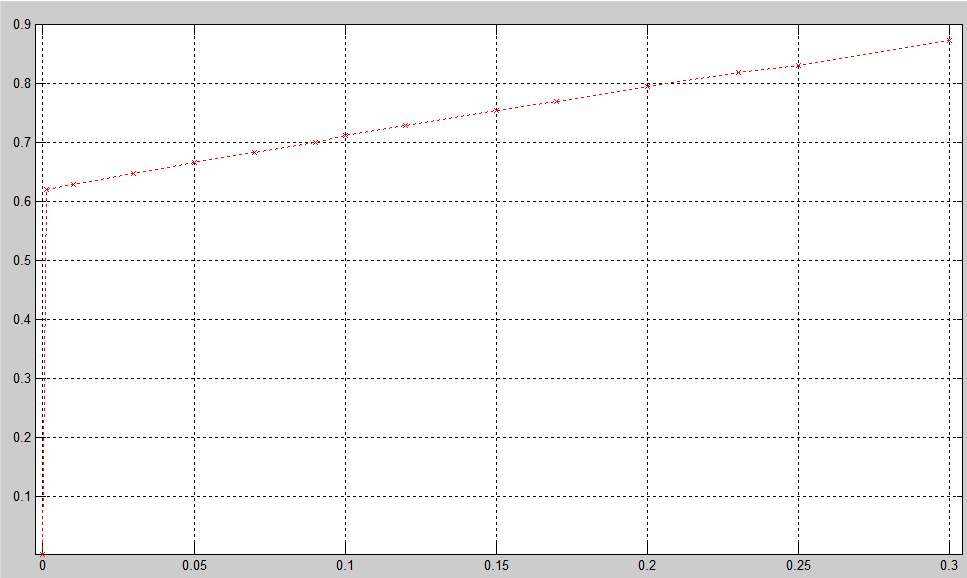


Рис.3.3 - Залежності P_{FA} та P_D для одного приймача

Як видно з рисунку 3.3, при ймовірності P_{FA} = 0.15, ймовірність виявлення P_D = 0.75. Надана ймовірність у деяких системах може бути недостатньою.

Для збільшення надійності аутентифікації об'єкту, було здійснено оцінку об'єкту, що верифікується, по відношенню не до одного приймача, а к декільком, як зображено на рисунку 3.4. Вузли №10, 12 й 13 – приймачі, а вузли №1-9 – передавачі.

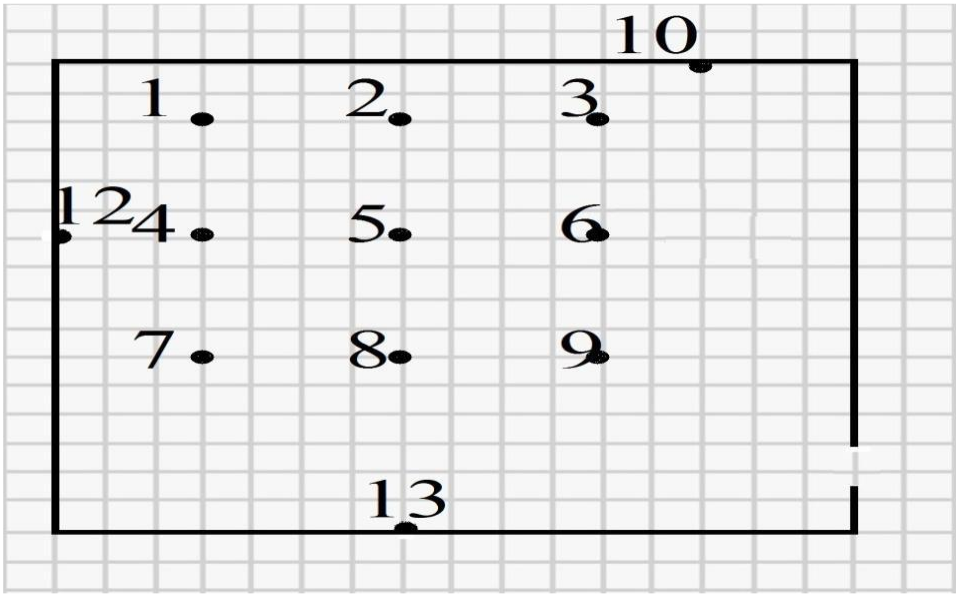


Рис.3.4 - Карта розташування пристроїв для декількох приймачів

Визначено множину J як множину приймачів, що беруть участь у спільному прийомі від передавачів i.

Алгоритм було побудовано наступним чином:

- Кожний приймач $j \in J$ записує історію $H_{i,j}$ довжиною N-1 й обчислює середню різницю $\sigma_{i,j}$.
- Кожний приймач $j \in J$ записує нове N-є значення $h^{(N)}$ й обчислює евклідову відстань $d_{i,j}$.
- Далі знаходиться мінімальне $d_{i,j}$ між усіма приймачами.

$$d_{i,J} = \frac{1}{|J|}\sum_{j \in J} d_{i,j}$$

- Результат $d_{i,j}$ порівнюється з пороговим значенням $\gamma > 0$, якщо

  $d_{i,j}$ більше за порога, то центральний вузол приймає рішення, що нове значення відповідає місцезнаходженню зловмисника. В іншому випадку, він вирішує, що нове значення відповідає тому ж самому місцю передавача, як і раніше, тоді кожний приймач додає $h_{i,j}^{(N)} = h^{(N)}$ до своєї історії (i, J).

Різниця між цим алгоритмом й тим, що було розглянуто раніше, у тому, що ми об’єднуємо сигналі з різних приймачів, а рішення приймає центральний вузол J.

Далі буде зрівняно $d_{i,j}$ з $d_{i,j}^{(N)}$. При цьому, також може бути дійсною кожна з цих двох гіпотез:

- H0: $d_{i,j} = d_{i,j}{}^{(N)}$, тобто об'єкт істинний;
- H1: $d_{i,j} = d_{i\text{-}i',j}$, тобто об'єкт помилковий.

Для цих припущень можна ввести ймовірності:

- P_{FA} - ймовірність помилкової тривоги;
- P_D - ймовірність виявлення.

Для гауссовського закону розподілу випадкової величини $d_{i,j}$, можна ці величини записати наступним чином:

$$P_{FA} = \sqrt{\frac{1}{2\pi\sigma^2}} \int_{\gamma}^{\infty} e^{\left(-\frac{1}{2\sigma^2}\left(x-d_{i,J}^{(N)}\right)^2\right)} dx$$

$$P_D = \sqrt{\frac{1}{2\pi\sigma^2}} \int_{\gamma}^{\infty} e^{\left(-\frac{1}{2\sigma^2}\left(x-d_{i-i',J}\right)^2\right)} dx$$

Далі проаналізовано алгоритм, що було представлено вище, для того, щоб перевірити це твердження, використовуючи експериментальні дані.

Отримано нашу базу даних поточних вимірювань для кожного приймача.

База даних приймача №10:

$$H_{i,10}^{(1)} = \begin{bmatrix} 43.892 & 45.419 & 47.634 \\ 47.472 & 43.865 & 43.817 \\ 48.783 & 45.527 & 47.820 \end{bmatrix} \quad H_{i,10}^{(2)} = \begin{bmatrix} 43.746 & 43.829 & 45.288 \\ 45.312 & 45.813 & 47.836 \\ 44.458 & 42.732 & 48.797 \end{bmatrix}$$

$$H_{i,10}^{(3)} = \begin{bmatrix} 46.784 & 44.859 & 45.651 \\ 44.774 & 43.915 & 42.062 \\ 45.388 & 46.256 & 45.469 \end{bmatrix} \quad H_{i,10}^{(4)} = \begin{bmatrix} 46.896 & 45.008 & 47.407 \\ 44.577 & 46.333 & 43.449 \\ 44.414 & 43.659 & 41.922 \end{bmatrix}$$

$$H_{i,10}^{(5)} = \begin{bmatrix} 42.762 & 45.293 & 47.368 \\ 53.408 & 45.637 & 48.727 \\ 44.340 & 44.447 & 44.708 \end{bmatrix}$$

База даних приймача №12:

$$H_{i,12}^{(1)}=\begin{bmatrix}40.541 & 45.236 & 45.855\\ 48.647 & 44.693 & 43.444\\ 50.204 & 44.806 & 44.331\end{bmatrix} H_{i,12}^{(2)}=\begin{bmatrix}45.420 & 42.830 & 44.785\\ 45.625 & 44.746 & 46.472\\ 43.876 & 44.364 & 45.095\end{bmatrix}$$

$$H_{i,12}^{(3)}=\begin{bmatrix}47.453 & 44.330 & 47.237\\ 45.176 & 44.741 & 45.003\\ 44.438 & 44.970 & 43.356\end{bmatrix} H_{i,12}^{(4)}=\begin{bmatrix}40.776 & 41.719 & 46.748\\ 46.482 & 44.247 & 44.809\\ 43.747 & 46.408 & 44.953\end{bmatrix}$$

$$H_{i,12}^{(5)}=\begin{bmatrix}46.996 & 40.988 & 43.306\\ 44.645 & 47.881 & 48.820\\ 45.364 & 39.104 & 47.834\end{bmatrix}$$

База даних приймача №13:

$$\mathrm{H}_{\mathrm{i,13}}^{(1)}=\begin{bmatrix}45.574 & 44.734 & 45.154\\ 46.395 & 42.681 & 41.991\\ 49.516 & 45.962 & 45.514\end{bmatrix} \mathrm{H}_{\mathrm{i,13}}^{(2)}=\begin{bmatrix}45.175 & 42.581 & 45.045\\ 46.757 & 46.195 & 47.249\\ 45.839 & 44.345 & 45.721\end{bmatrix}$$

$$\mathrm{H}_{\mathrm{i,13}}^{(3)}=\begin{bmatrix}48.259 & 43.310 & 44.776\\ 44.872 & 45.857 & 49.818\\ 42.264 & 45.396 & 44.656\end{bmatrix} \mathrm{H}_{\mathrm{i,13}}^{(4)}=\begin{bmatrix}42.709 & 46.469 & 44.193\\ 45.035 & 43.507 & 44.840\\ 44.642 & 46.556 & 42.519\end{bmatrix}$$

$$\mathrm{H}_{\mathrm{i,13}}^{(5)}=\begin{bmatrix}41.890 & 44.801 & 42.152\\ 47.979 & 44.962 & 48.796\\ 44.878 & 44.856 & 52.370\end{bmatrix}$$

Для того, щоб знайти відстані між поточним станом й базою даних за формулою (3).

Для цього, було перебрано усі значення виразу $|h-g|$ за формулою (2). $|h-g|$ - це різниця значень параметрів між парами вузлів у поточному вимірі, де g – це поточний стан вузла, а h – поточні значення інших вузлів.

Було записано різниці $|h - g|$ для кожного приймача №10, №12, №13 у таблиці (3.7. – 3.9.) з відповідністю до пар вузлів.

Таблиця 3.7 - Різниця $|h - g|$ й середня різниця $\sigma_{i,j}$ для N-1 вимірів приймача №10

Пари вузлів	Різниця |h – g| для вимірів:				$\sigma_{i,j}$
	1	2	3	4	
12	1.637	0.195	2.213	1.998	0.563
13	3.850	1.653	1.244	0.622	0.688
14	3.631	1.677	2.121	2.423	0.772
15	0.138	2.168	2.978	0.674	0.572
16	0.186	4.228	4.833	3.558	1.141
17	4.933	0.823	1.435	2.583	0.812
18	1.768	1.125	0.678	3.348	0.645
19	3.988	5.162	1.454	4.986	1.383
23	2.348	1.604	0.819	2.451	0.687
24	2.169	1.593	0.197	0.543	0.449
25	1.667	2.203	1.176	1.436	0.596
26	1.713	4.145	3.001	1.667	0.944
27	2.456	0.780	0.641	0.988	0.537
28	0.280	2.223	1.547	1.456	0.432
29	2.516	4.957	0.722	3.197	1.107

34	0.275	0.157	0.988	2.934	0.432
35	4.002	0.637	1.847	1.185	0.618
36	3.997	2.687	3.657	4.210	1.273
37	1.321	0.942	0.374	3.134	0.547
38	2.223	2.667	0.716	3.858	0.863
39	0.243	3.708	0.293	5.596	0.891
45	3.718	0.623	0.915	1.867	0.661
46	3.769	2.667	2.823	1.239	0.948
47	1.432	0.987	0.725	0.274	0.356
48	2.003	2.687	1.593	1.113	0.688
49	0.478	3.596	0.758	2.766	0.617
56	0.151	2.162	1.934	2.995	0.580
57	4.901	1.456	1.584	2.234	0.917
58	1.773	3.182	2.456	2.789	0.915
59	4.104	3.231	1.667	4.522	1.189
67	4.967	3.516	3.437	1.078	1.155
68	1.823	5.242	5.102	0.321	1.008

69	4.115	1.142	3.518	1.638	0.997
78	3.367	1.837	0.988	2.546	0.660
79	3.369	4.446	0.191	2.848	0.767
89	2.360	6.176	0.898	1.981	0.998

Таблиця 3.8 - Різниця | $h - g$ | й середня різниця $\sigma_{i,j}$ для N-1 вимірів приймача №12

Пари вузлів	Різниця |h – g| для вимірів:				$\sigma_{i,j}$
	1	2	3	4	
12	4.719	2.637	3.234	1.004	0.997
13	5.426	0.746	0.327	6.101	1.123
14	8.218	0.316	2.388	5.808	1.459
15	4.263	0.785	2.816	3.582	0.978
16	2.998	1.163	2.555	4.144	0.980
17	9.778	1.655	3.127	3.103	1.566
18	4.376	1.166	2.595	5.743	1.230
19	3.820	0.436	4.113	5.288	1.142
23	0.734	2.118	3.101	5.135	0.987
24	3.522	2.879	0.989	4.864	1.143
25	0.654	2.109	0.522	2.639	0.560
26	1.870	3.753	0.784	3.112	0.877

27	5.109	1.159	0.219	2.129	0.734
28	0.570	1.657	0.751	4.798	0.718
29	1.230	2.365	1.121	3.345	0.723
34	2.890	0.967	2.172	0.377	0.543
35	1.278	0.178	2.560	2.604	0.628
36	2.514	1.789	2.356	2.132	0.734
37	4.450	1.109	2.990	3.112	1.142
38	1.267	0.532	2.379	0.453	0.450
39	1.678	0.423	3.992	1.890	0.774
45	4.129	0.920	0.546	2.346	0.738
46	5.307	0.958	0.284	1.784	0.765
47	1.669	1.803	0.849	2.847	0.675
48	3.952	1.372	0.317	0.185	0.559
49	4.427	0.670	1.980	1.629	0.794
56	1.345	1.837	0.373	0.673	0.428
57	5.623	0.980	0.414	0.611	0.637
58	0.224	0.492	0.312	2.272	0.390
59	0.473	0.430	1.496	0.809	0.243
67	6.871	3.102	0.677	1.175	0.951

68	1.473	2.209	0.145	1.689	0.536
69	0.998	1.490	1.758	0.255	0.449
78	5.435	0.599	0.643	2.772	0.868
79	5.985	1.320	1.192	1.314	0.893
89	0.587	0.842	1.715	1.566	0.476

Таблиця 3.9 - Різниця | $h - g$ | й середня різниця $\sigma_{i,j}$ для N-1 вимірів приймача №13

Пари вузлів	Різниця |h – g| для вимірів:				$\sigma_{i,j}$
	1	2	3	4	
12	0.952	2.675	5.104	3.870	1.123
13	0.523	0.242	3.593	1.595	0,570
14	0.934	1.693	3.498	2.437	0.787
15	2.913	1.131	2.502	0.810	0.617
16	3.695	2.184	1.667	2.233	0.809
17	4.103	0.775	6.109	2.109	1.155
18	0.499	0.931	2.974	4.108	0.770
19	0.172	0.657	3.617	0.213	0.409
23	0.542	2.575	1.577	2.387	0.663

24	1.773	4.288	1.678	1.545	0.837
25	2.164	3.725	2.678	3.106	1.029
26	2.864	4.779	6.619	1.718	1.351
27	4.894	3.365	1.157	1.938	1.001
28	1.334	1.875	2.199	0.234	0.560
29	1.390	3.252	1.445	4.142	0.879
34	1.352	1.823	0.106	0.953	0.435
35	2.584	1.267	1.191	0.797	0.567
36	3.276	2.307	5.151	0.758	1.264
37	4.474	0.812	2.617	0.517	0.788
38	0.913	0.800	0.790	2.584	0.494
39	0.470	0.788	0.240	1.784	0.347
45	3.826	0.674	1.108	1.639	0.677
46	4.505	0.519	5.090	0.276	0.957
47	3.244	1.100	2.719	0.408	0.687
48	0.567	2.524	0.635	1.759	0.528
49	0.992	1.147	0.318	2.616	0.498
56	0.786	1.165	4.109	1.444	0.697
57	6.937	0.467	3.617	1.246	1.223

58	3.393	1.960	0.576	3.275	0.897
59	2.944	0.585	1.308	1.113	0.569
67	7.637	1.520	7.665	1.009	1.423
68	4.189	2.990	4.544	1.936	1.134
69	3.634	1.638	5.243	2.439	1.155
78	3.665	1.549	3.241	2.134	0.990
79	4.114	0.229	2.419	2.233	0.667
89	0.567	1.487	0.841	4.257	0.443

Була розрахована евклідова відстань між поточним станом об'єкту й базою даних. Для кожного вузла було обрано варіант з мінімальною відстанню. У таблиці 3.10. показано параметр $d_{i,j}$ для кожного приймача, а також результат середньої відстані, що було обчислено за формулою (6). Таблиця 3.10- Різниця $|h - g|$ й середня різниця $\sigma_{i,j}$ для N-1 вимірів приймача №14

Пари вузлів	Різниця |h – g| для вимірів:				$\sigma_{i,j}$
	1	2	3	4	
12	4.719	2.637	3.234	1.004	0.997
13	5.426	0.746	0.327	6.101	1.123
14	8.218	0.316	2.388	5.808	1.459
15	4.263	0.785	2.816	3.582	0.978
16	2.998	1.163	2.555	4.144	0.980
17	9.778	1.655	3.127	3.103	1.566

18	4.376	1.166	2.595	5.743	1.230
19	3.820	0.436	4.113	5.288	1.142
23	0.734	2.118	3.101	5.135	0.987
24	3.522	2.879	0.989	4.864	1.143
25	0.654	2.109	0.522	2.639	0.560
26	1.870	3.753	0.784	3.112	0.877
27	5.109	1.159	0.219	2.129	0.734
28	0.570	1.657	0.751	4.798	0.718
29	1.230	2.365	1.121	3.345	0.723
34	2.890	0.967	2.172	0.377	0.543
35	1.278	0.178	2.560	2.604	0.628
36	2.514	1.789	2.356	2.132	0.734
37	4.450	1.109	2.990	3.112	1.142
38	1.267	0.532	2.379	0.453	0.450
39	1.678	0.423	3.992	1.890	0.774
45	4.129	0.920	0.546	2.346	0.738
46	5.307	0.958	0.284	1.784	0.765
47	1.669	1.803	0.849	2.847	0.675
48	3.952	1.372	0.317	0.185	0.559

49	4.427	0.670	1.980	1.629	0.794
56	1.345	1.837	0.373	0.673	0.428
57	5.623	0.980	0.414	0.611	0.637
58	0.224	0.492	0.312	2.272	0.390
59	0.473	0.430	1.496	0.809	0.243
67	6.871	3.102	0.677	1.175	0.951
68	1.473	2.209	0.145	1.689	0.536
69	0.998	1.490	1.758	0.255	0.449
78	5.435	0.599	0.643	2.772	0.868
79	5.985	1.320	1.192	1.314	0.893
89	0.587	0.842	1.715	1.566	0.476

Таблиця 3.11. Евклідові відстані для N-1 вимірів приймачів №10, №11, №12

Пари вузлів	Різниця |h – g| для вимірів:			$d_{i,J} = \frac{1}{\|J\|}\sum_{j\in J} d_{i,j}$	
	10	12	13	J = 2	J = 3
12	3.113	0.335	0.480	1.773	1.342
13	0.929	2.109	1.313	1.565	1.484
14	8.359	0.663	0.514	4.517	3.188

15	2.534	0.577	0.470	1.530	1.208
16	1.889	1.682	0.710	1.776	1.457
17	0.677	0.143	0.396	0.413	0.309
18	1.149	1.394	0.588	1.270	1.308
19	0.752	0.432	12.318	0.606	4.186
23	3.519	0.654	0.889	2.108	1.689
24	23.778	0.432	2.143	13.001	8.900
25	0.563	5.993	0.354	3.208	2.220
26	4.109	4.788	2.890	4.465	3.596
27	1.230	0.209	0.234	0.710	0.626
28	1.372	4.404	0.389	2.888	2.109
29	0.274	4.337	8.109	2.305	4.134
34	18.900	0.393	8.814	8.709	9.329
35	0.145	1.357	0.296	0.746	0.696
36	0.980	3.321	4.108	1.760	2.508
37	2.289	0.644	0.262	1.465	1.119
38	1.230	17.809	0.318	9.109	6.125
39	0.855	1.301	27.670	0.990	11.899
45	0.673	1.335	0.109	0.999	0.756

46	1.670	0.375	2.549	0.993	1.500
47	1.189	0.445	0.122	0.753	0.549
48	0.337	13.649	0.139	6.993	4.705
49	0.222	1.209	12.870	0.761	5.375
56	4.304	11.990	4.547	8.643	7.209
57	0.647	1.143	1.109	0.890	0.980
58	0.765	23.401	1.484	10.124	7.976
59	0.848	14.337	12.576	7.176	9.998
67	0.513	0.408	0.129	0.556	0.509
68	0.783	10.409	0.125	5.587	3.742
69	1.129	4.144	2.556	2.669	2.631
78	0.123	6.246	0.264	3.189	2.247
79	0.490	3.134	4.425	1.809	2.507
89	1.109	4.115	9.301	2.564	5.174

Таблиця 3.12 - Значення ймовірностей P_{FA}, P_D для j =1, 2 й 3 (приймачей)

P_{FA}	P_D (j =1)	P_D (j = 2)	P_D (j =3)
0.001	0.532	0.858	0.8860
0.01	0.539	0.860	0.8863
0.03	0.559	0.862	0.8866

0.05	0.578	0.865	0.8870
0.07	0.595	0.868	0.8873
0.09	0.512	0.871	0.8875
0.1	0.523	0.872	0.8876
0.12	0.530	0.873	0.8876
0.15	0.565	0.876	0.8877
0.17	0.581	0.878	0.8882
0.2	0.597	0.880	0.8882
0.23	0.531	0.882	0.8885
0.25	0.532	0.884	0.8885
0.3	0.585	0.885	0.8887

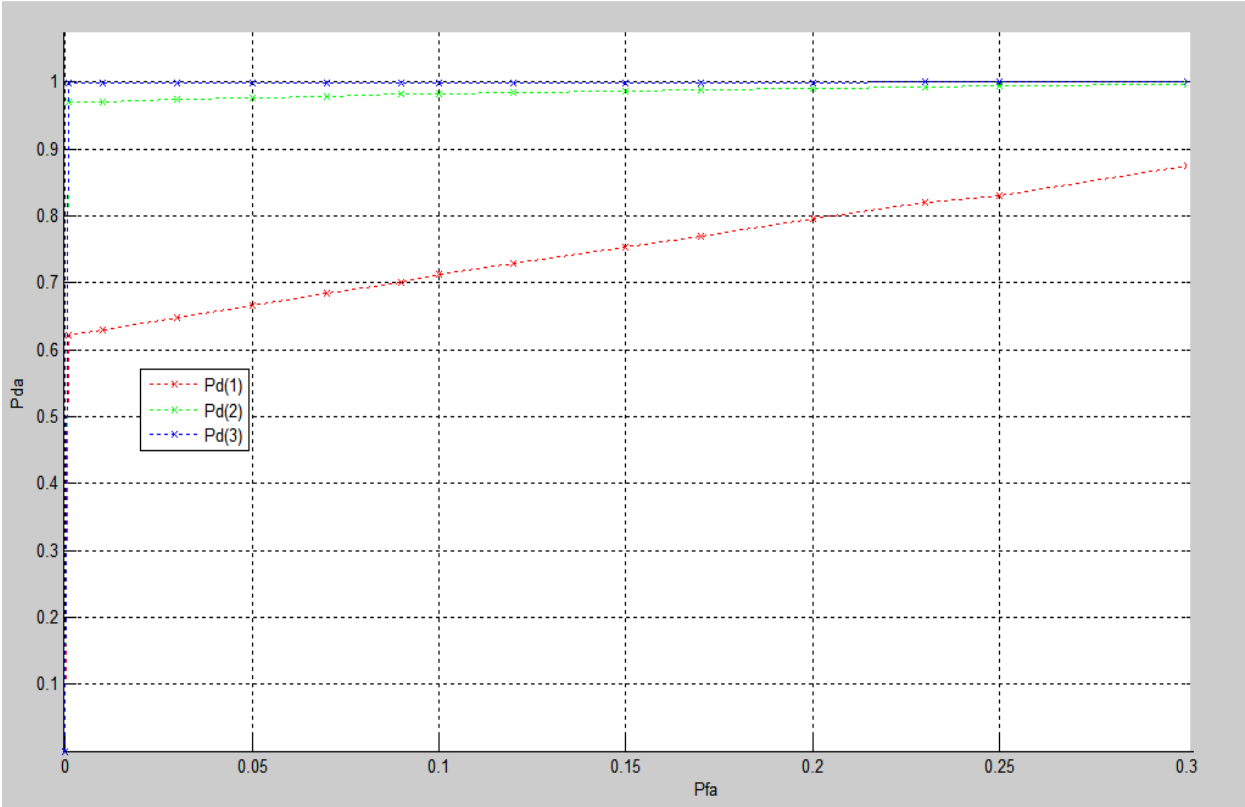


Рис.3.5 - Залежність P_{FA} та P_D для: P_D (1) - одного приймача, P_D (2) – двох приймачів, P_D (3) - трьох приймачів

У таблиці 3.12 розміщено ймовірності виявлення для одного, двох та трьох приймачів, графік залежності P_{FA} від P_D, розрахованих при різних γ. Дані залежності для наочності зображено на малюнку 3.5.

Система аутентифікації, що включає в себе три приймача, дозволяє довести вірогідність виявлення до 0.9977 при ймовірності помилкової тривоги 0.03. Таким чином, подальше збільшення кількості приймачів, можна вважати недоцільним, а систему з трьома приймачами вважати оптимальним рішенням.

ВИСНОВОК

Однією з найбільш важливих завдань інформаційної безпеки є забезпечення безпечної аутентифікації користувачів. Аутентифікація користувачів - це процес підтвердження особи. Одним з нових напрямків в даній сфері, це аутентифікація користувачів на основі розташування. Розвиток даного напряму в даний час має особливе місце для різних пристроїв в галузі бездротових мереж. Щоб забезпечити аутентифікацію без пароля, в даній дисертації розроблений і промодельований спосіб аутентифікації на основі розташування.

Для здійснення аутентифікації створюється база даних вимірювань «радіовідбитків каналів». Обчислюється мінімальне евклідова відстань між поточним виміром і історією. Дане значення порівнюється з граничним значенням і визначається легітимність користувача. Дано оцінки ймовірності виявлення і помилкової тривоги для систем з одним і кількома приймачами. Для вибору порогового значення використовувався критерій Неймана-Пірсона.

Для реалізації алгоритму і його моделювання розроблено імітаційну модель в системі Matlab. В якості моделі сигналу іспользовалсяOFDM-сигнал, що відповідає стандарту IEEE 802.11b, для обліку перешкод в каналі використовувалася модель каналу з АБГШ. За допомогою даної моделі проводилася оцінка надійності алгоритму аутентифікації при появі в мережі в нелегітимного користувача.

Проведено моделювання алгоритму на прикладі аутентифікації дев'яти користувачів, розташованих в приміщенні на відстані один від одного 2 м.

На основі результатів моделювання і розрахунків показано, що при використанні одного приймача, при ймовірності помилкової тривоги 0.1, ймовірність правильного виявлення дорівнюватиме 0.7. Зі збільшенням кількості приймачів ймовірність правильного виявлення при тій же ймовірності помилкової тривоги збільшується до 0.98 з двома приймачами, і 0.99 з двома приймачами. Тим самим, більш висока надійність аутентифікації, буде досягнута при використанні двох або трьох приймачів.

- проаналізовано існуючи методи аутентифікації користувача на фізичному рівні взаємодії мережі.

- наведено моделювання алгоритму на прикладі аутентифікації об'єктів, що розташовані в сучасному офісі.
- отримані залежності ймовірності виявлення об'єкта від ймовірності помилкової тривоги. На основі результатів моделювання і розрахунків, показано, що аутентифікація з одним приймачем досягає ймовірності 0.87 при ймовірності помилкового об'єкта 0.3.
- розроблено алгоритм і проведено його моделювання для системи аутентифікації, що включає 2 і 3 приймача. Так, для трьох приймачів можна отримати ймовірність виявлення 0.9977 при ймовірності помилкової тривоги 0.03.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Блэк У. Интернет: протоколы безопасности. Учебный курс. СПб.: Питер, 2001. – С. 13-31.

2. Беспроводные сети Wi-Fi. Аутентификация в беспроводных сетях [Електронний ресурс] – Режим доступу до ресурсу: http://www.intuit.ru/studies/courses/1004/202/lecture/5252?page=1.

3. Комп'ютерні мережі: навчальний посібник [Текст] / Азаров О.Д., Захарченко С.М., Кадук О.В., Орлова М.М., Тарасенко В.П..-Вінниця: ВНТУ. - 2013. - 371 с.

4. Э. Немет, Г. Снайдер, Т. Хейн, Б. Уэйли. Unix и Linux: руководствосистемного администратора, 4-е изд. : Пер. с англ. – М. : ООО «И.Д. Вильямс», 2012. – 1312 с.

5. Jesin A. Packet Tracer Network Simulator. – Packt Publishing, 2014.

6. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010. – 944 с.

7. С. Ганус. MLAG [Електронний ресурс]. – 2013. – Режим доступу: http://www.solidex.by/blogs/notes/mlag.php

8. Н. Самойленко. Безопасность канального уровня [Електронний ресурс]. – 2010. – Режим доступу: http://xgu.ru/wiki/Безопасность_канального_уровня

9. Н. Олифер. Резервирование соединений в локальных сетях [Електронний ресурс]. – 2002. – Режим доступу: http://www.osp.ru/lan/2002/01/135732/

10 . Отчет о количестве сайтов в сети интернет // Netcraft [Электронный ресурс]. – Режим доступа: http://techno.bigmir.net/technology/1577735-Kolichestvo-sajtov-v-internete-perevalilo-za-milliard, свободный (дата обращения 20.04.2016).

11. Кияев В., Граничин О. Безопасность информационных систем // НОУ “ИНТУИТ”, 2016.

12. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа // Наука и Техника, Санкт-Петербург, 2004.

13. 2015 Cyber Security Survey: Major Australian Business // Australian Government, Australian Cyber Security Centre.

14. Сабанов А.Г., Шелупанов А.А., Мещеряков Р.В. Требования к системам аутентификации по уровням строгости // УДК 004.089 [Электронный ресурс]. – Режим доступа: http://new.elib.altstu.ru/journals/Files/pv2012_2_1/pdf/061sabanov.pdf, свободный (дата обращения 23.04.2016).

15. Сабанов А.Г. Об уровнях аутентификации в информационном обществе // Защита информации. INSIDE № 2’2012.

16. Электронное правительство // [Электронный ресурс]. – Режим доступа: http://www.rostelecom.ru/projects/egov/about/, свободный (дата обращения 23.04.2016).

17. Homeland Security Presidential Directive. Policy for a Common Identification Standard for Federal Employees and Contractors. August 27, 2004. [Электронный ресурс]. – Режим доступа: https://www.dhs.gov/homeland-security-presidential-directive-12, свободный (дата обращения 24.04.2016)

18. Electronic Authentication Guideline // NISTSpecialPublication 800-63 April 2006 [Электронный ресурс]. – Режим доступа: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf, свободный (дата обращения 24.04.2016).

19. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа // Наука и Техника, Санкт-Петербург, 2004.

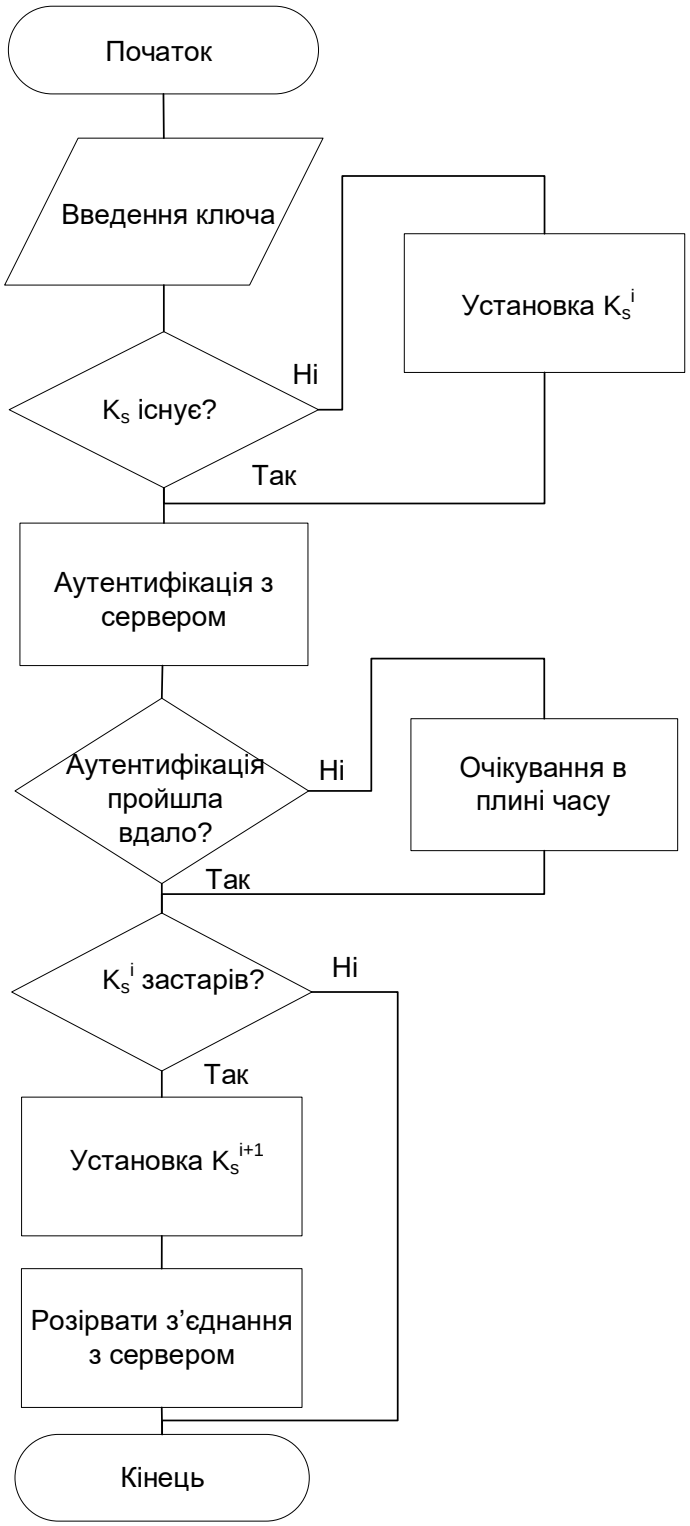
Додаток 1.

Копії графічних матеріалів

Системи ідентифікації та аутентифікації

Тупарєва В.А.

Схема алгоритму аутентифікації з загальним ключем

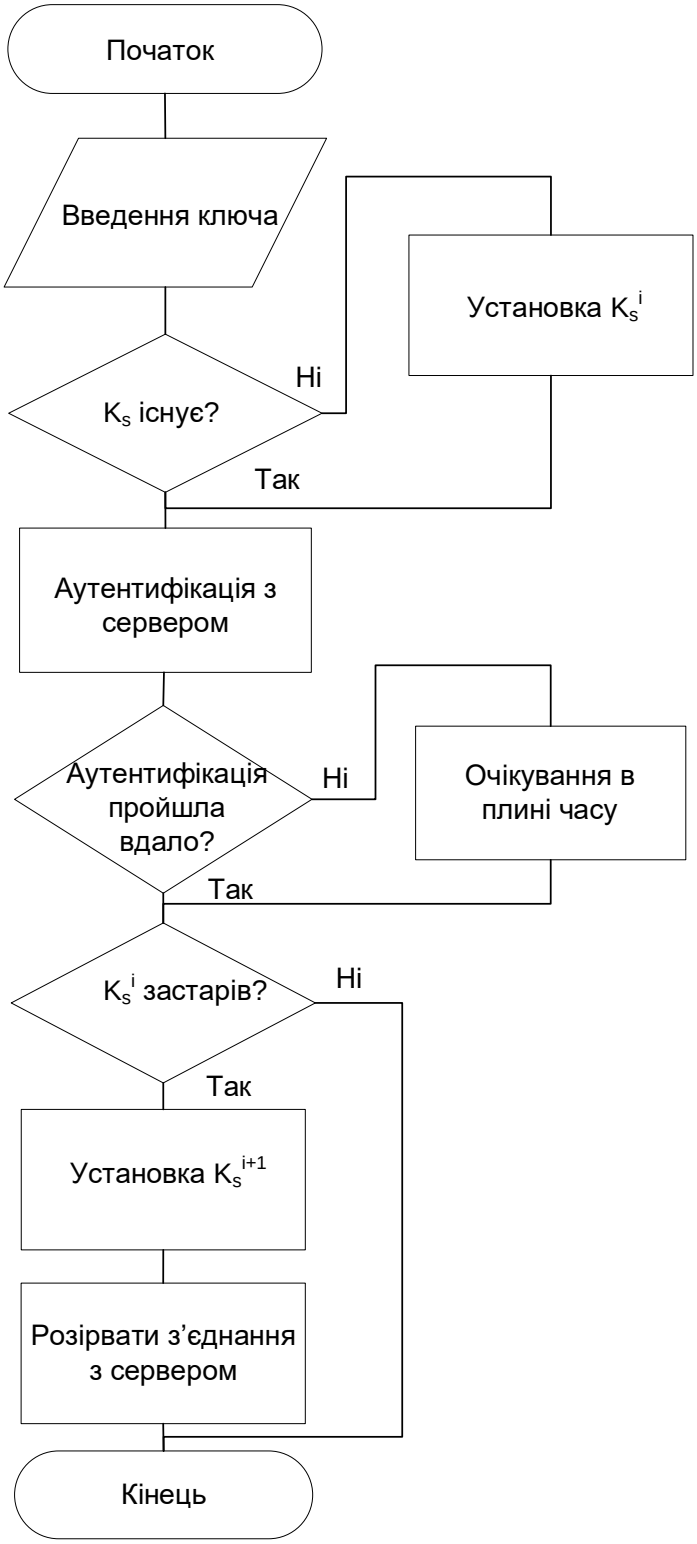


Тупарєва В.А.

Схема алгоритму аутентифікації за допомогою біометричних характеристик

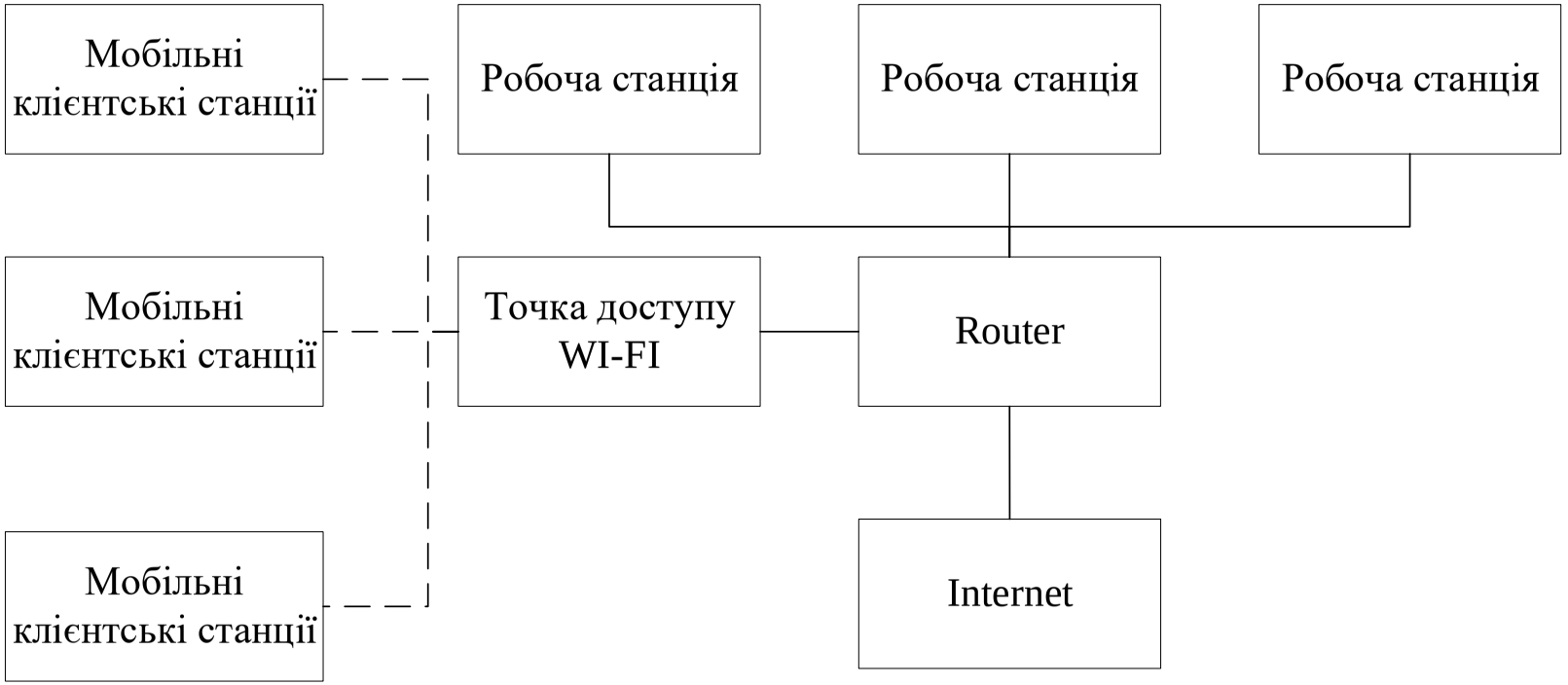
Тупарєва В.А.

Схема алгоритму аутентифікації з загальним ключем



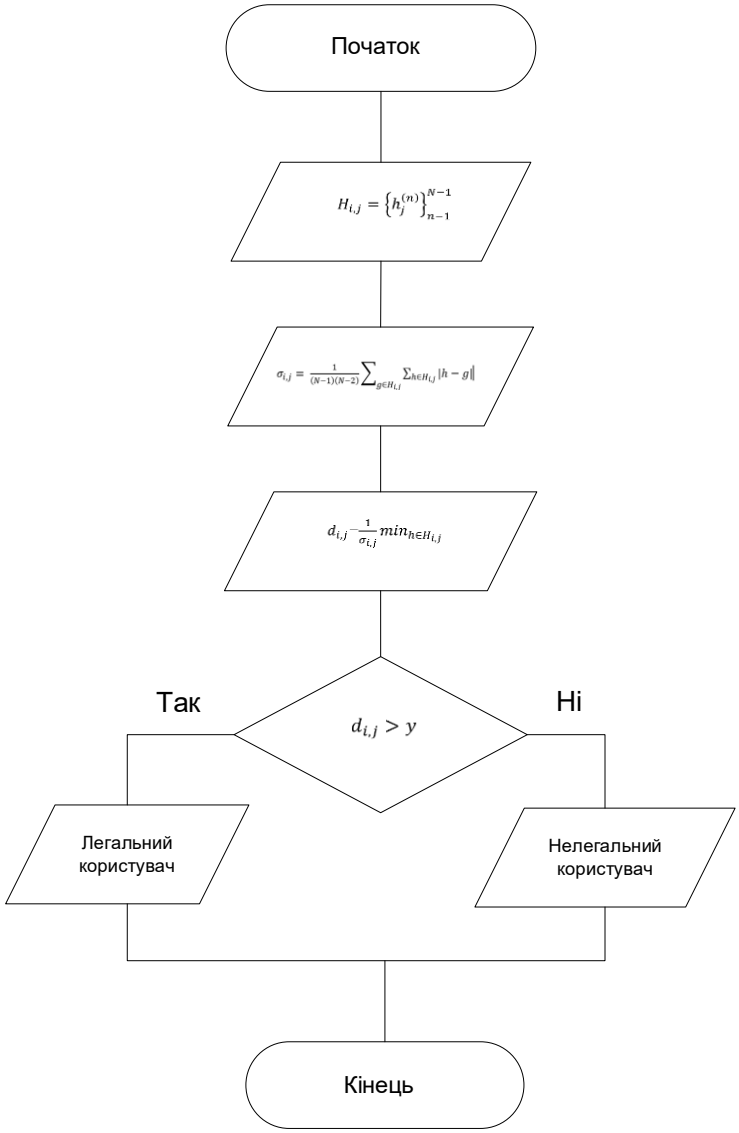
Тупарєва В.А.

Організація WI-FI мережі



Тупарєва В.А.

Блок-схема алгоритму аутентифікації



Тупарєва В.А.